UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* TARGET ACCOUNTS that were produced by Meta Platforms. Inc. and currently stored at FBI's Seattle office, more fully described in Attachment A	)	Case No. MJ24-435

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, incorporated by reference

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§§ 1343, 1349, and 1956(h)	Wire Fraud; Conspiracy to Commit Wire Fraud; and Conspiracy to Commit Money Laundering

The application is based on these facts:

✓ See affidavit of FBI Special Agent Ethan Via, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Ethan Via, Special Agent, FBI

Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 07/24/2024

Judge's signature

City and state: Seattle, Washington

Hon. Mary Alice Theiler, United States Magistrate Judge

Printed name and title

USAO: 2019R01037

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Ethan Via, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a search warrant authorizing the examination of all data, information, communications, and logs related to the following Facebook accounts:

- Facebook ID number 1626067687446970 with vanity name HashFlareGlobal;
- Facebook ID number100002183784122 with vanity name turygin; and
- Facebook ID number 1764433774 with vanity name Sergeit.pt

(hereinafter, the "TARGET ACCOUNTS"), which were stored at premises controlled by Meta Platforms, Inc. ("Meta"), a company located in Menlo Park, California; produced to investigators by Meta; and currently stored at the Federal Bureau of Investigation's office in Seattle, Washington.

2. I am employed as a Special Agent with the FBI and have been employed with the FBI since August 2003. I am currently assigned to the Seattle Field Division where I am a member of the Complex Financial Crime squad. I have received basic federal law enforcement training, including the training at the FBI Academy in Quantico, Virginia, as well as other specialized law enforcement training. Before my career as an FBI Special Agent, I was employed as a Certified Public Accountant for approximately three years and, as part of that employment, I examined financial information of clients to determine their accuracy and reliability.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

3. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; and communications with others who have personal knowledge of the events and circumstances described herein.

4. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1349 (Conspiracy to Commit Wire Fraud), 1343 (Wire Fraud), and 1956(h) (Conspiracy to Commit Money Laundering) will be found in the TARGET ACCOUNT.

PURPOSE OF AFFIDAVIT

5. This is an additional application for a search warrant for the TARGET ACCOUNTS. On or about April 6, 2022, U.S. Magistrate Judge Paula L. McCandlis issued a warrant for the TARGET ACCOUNTS (and other accounts not at issue here) in Case Number MJ22-136, which is attached and incorporated herein by reference.

6. The prior warrant was served on Meta on or about April 7, 2022. About three weeks later, on or about April 26, 2022, Meta produced the TARGET ACCOUNTS to the FBI. The FBI downloaded the materials, which was submitted into evidence on or about April 27, 2022, and provided a copy to the U.S. Attorney's Office in the Western District of Washington for upload to a document review software application.

7. Upon attempting to upload the materials for the TARGET ACCOUNTS into a document review software application, the case team learned that the TARGET ACCOUNTS were primarily in Russian and that the document review software application was incapable of translating the TARGET ACCOUNTS into English. In

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

addition, the complexity of the subject matter of the TARGET ACCOUNTS requiring translation precluded the use of FBI linguists as an efficient means of translation.

8. In October 2022, a grand jury sitting in this district returned an indictment charging the defendants, SERGEI POTAPENKO and IVAN TUROGIN, with violations of Title 18, United States Code, Sections 1349 (Conspiracy to Commit Wire Fraud), 1343 (Wire Fraud), and 1956(h) (Conspiracy to Commit Money Laundering) for their role in series of interrelated fraudulent solicitations related to virtual currency. *See United States v. Potapenko & Turogin*, CR22-185 RSL.

9. In or around June 2024, the case team learned that the FBI now had access to a software application capable of translating the TARGET ACCOUNTS into English. On June 24, 2024, I made a working copy of the TARGET ACCOUNTS and caused it to be transmitted to technicians at the FBI for upload into a software application for translation. Shortly thereafter, on or about July 1, 2024, the case team learned that the TARGET ACCOUNTS had been successfully translated into English. As of the date of this affidavit, the investigative team has not reviewed the translated contents of the TARGET ACCOUNTS.

10. In the approximately two years that have elapsed since the warrants in MJ22-136 were signed, the FBI has not acquired any additional information that would undermine the finding of probable cause to search the TARGET ACCOUNTS made by Judge Paula L. McCandlis in MJ22-136.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

11. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the materials to be searched are already in the FBI's possession, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. Accordingly, by this affidavit and warrant, I seek authority for the government to search all of the items specified in Attachment A (attached hereto and incorporated by reference herein) to the warrant, and specifically to seize all of the data, documents and records that are identified in Attachment B (attached hereto and incorporated by reference herein).

ETHAN VIA, Affiant
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on 24th day of July, 2024.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Accounts to be Searched

All data, information, communications, and logs related to the following Facebook account:

- Facebook ID number 1626067687446970 with vanity name HashFlareGlobal;
- Facebook ID number100002183784122 with vanity name turygin; and
- Facebook ID number 1764433774 with vanity name sergeit.pt

(collectively, the "Accounts"), which were stored at premises controlled by Meta Platforms, Inc., a company located in Menlo Park, California; produced to investigators by Meta Platforms, Inc.; and are currently stored at the Federal Bureau of Investigation's office in Seattle, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Information to be Seized by the Government

All records on the Accounts described in Attachment A that relate to violations of Title 18, United States Code, Sections 1349 (Conspiracy to Commit Wire Fraud), 1343 (Wire Fraud), and 1956(h) (Conspiracy to Commit Money Laundering), those violations occurring after April 2015, including information pertaining to the following matters:

a. Items, records, or information related to the operation of a cryptocurrency cloud mining Ponzi scheme;

b. Items, records, or information related to cryptocurrency mining, the advertisement, manufacture and sale of mining equipment, or the advertisement and sale of cloud mining contracts;

c. Items, records, or information related to the termination of mining contracts and the profitability of cloud mining;

d. Items, records, or information related to purchases of cloud mining equipment, including communications with the companies Jeltan Trading, Dalmeron Projects, Dalmeron Invest, Keleta UAB, Bitmain, Bitfury, and Inno3d;

e. Items, records, or information related to the transfer, purchase, sale, or disposition of cryptocurrency;

f. Items, records, or information related to communications with HASHFLARE or HASHCOINS investors, including complaints by investors or requests for return of funds;

g. Items, records, or information related to the advertisement of HASHFLARE or HASHCOINS' services;

h. Items, records, or information related to the owners, operators, employees, locations, assets, and business purpose of the companies HASHCOINS OU, HASHCOINS TRADE OU, HASHCOINS LP, HASHFLARE LP, Burfa Capital OU, Burfa Media OU, Burfa Real Estate OU, Burfa Tech OU, Burfa Trade OU, Burfa Invest OU, Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, Polybius Fintech MidCo OU, Dalmeron Projects LP, Jeltan Trading, Dalmeron Invest, Keleta UAB, and OSOM Finance (collectively, the "SUBJECT ENTITIES");

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. Items, records, or information related to the use, creation, or operation of the "SUBJECT ENTITIES," including business plans and strategies, and the anticipated success, failure, or general validity thereof;

j. Items, records, or information related to the operation of hashflare.io, burfa.com, polybius.io, dalmeron.com, or hashcoins.com;

k. Items, records, or information concerning financial transactions associated with the operation of the SUBJECT ENTITIES, including bank accounts held by the SUBJECT ENTITIES, transfers of funds by the SUBJECT ENTITIES, expenditures of money or wealth, bank statements and other financial statements, and cryptocurrency holdings;

l. Items, records, or information related to cryptocurrency mining groups, cryptocurrency public keys or addresses, cryptocurrency private keys, representations of cryptocurrency wallets or their constitutive parts, to include "recovery seeds" and "root keys," which may be used to regenerate a wallet;

m. Items, records, or information related to the salaries or earnings of individuals employed by the SUBJECT ENTITIES;

n. Items, records, or information related to the payment or calculation of recruitment bonuses paid to HASHFLARE and HASHCOINS investors;

o. Items, records, or information related to receipt of investor money, including the amount, purpose of the investment, and plans for spending that money;

p. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

q. Evidence indicating the account owner's state of mind as it relates to the crime under investigation; and

r. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

///

///

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys to the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ORIGINAL AFFIDAVIT AND SEARCH WARRANT MJ22-136

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Andrew Cropcho, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May of 2018. I am currently assigned to the Seattle Field Office. My primary duties include investigating violations of Federal law, including corporate fraud, securities fraud, government program fraud, and healthcare fraud. Part of those duties include investigating instances of wire fraud being used for financial gain at the expense of others. Before my career as an FBI Special Agent, I was employed by a large public accounting firm for over three years and, as part of my employment, I examined financial information of clients to determine their accuracy, reliability, and sources.

2. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein including, but not limited to, the victims in this investigation; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

3. I make this affidavit in support of an application for a search warrant for information associated with certain accounts (collectively, "TARGET ACCOUNTS") that are stored at premises controlled by the electronic communications service and/or remote computer service providers ("Provider(s)"), referenced below. The information to be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

searched is described in the following paragraphs and in Attachments A, which are incorporated herein. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the following:

a. **Twitter, Inc.** ("Twitter"), located at 1355 Market Street, Suite 900, San Francisco, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-1, pertaining to the following accounts (collectively the "**TWITTER ACCOUNTS**") identified in Attachment A-1:

- **ID 176428871/Username "turygin" ("TWITTER 1")**
- **ID 2942255620/Username "Hashflare" ("TWITTER 2")**
- **ID 806404856370102272/Username "PolybiusEU" ("TWITTER 3")**

b. **Meta Platforms, Inc.** ("Meta"), located at 1601 Willow Road, Menlo Park, California, parent company of **Facebook**, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-2, pertaining to the following accounts (collectively the "**FACEBOOK ACCOUNTS**") identified in Attachment A-2:

- **ID 1626067687446970/Vanity Name "HashFlareGlobal" ("FACEBOOK 1")**
- **ID 100002183784122/Vanity Name "turygin" ("FACEBOOK 2")**
- **ID 1764433774/Vanity Name "sergei.pt" ("FACEBOOK 3")**

c. **Slack Technologies, Inc.** ("Slack"), located at 500 Howard Street, San Francisco, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-3, pertaining to the following account(s) (collectively the "**SLACK ACCOUNTS**") identified in Attachment A-3:

- **Workspace name "BDC"/Workspace URL "borealisdc.slack.com" ("SLACK 1")**

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

- **Workspace name "HashCoins"/Workspace URL "hashcoins.slack.com" ("SLACK 2")**
- **Workspace name "Polybius"/Workspace URL "polybiusbank.slack.com" ("SLACK 3")**
- **Workspace name "Polybius"/Workspace URL "polybius-io.slack.com" ("SLACK 4")**

d. Zendesk, Inc. ("Zendesk"), located at 989 Market Street, San Francisco, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-4, pertaining to the following account, identified in Attachment A-4:

- **Account Number 700253/Account Name "hashflare" ("ZENDESK ACCOUNT")**

e. Dropbox, Inc. ("Dropbox"), located at 1800 Owens Street, Suite 200, San Francisco, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-5, pertaining to the following accounts (collectively the **"DROPBOX ACCOUNTS")** identified in Attachment A-5:

- **Account e-mail address sergei.potapenko@gmail.com/User ID 10722656/Full Name Sergei Potapenko ("DROPBOX 1")**
- **Account e-mail address sergei@burfa.com/User ID 995978848/Full Name Sergei Potapenko ("DROPBOX 2")**
- **Account e-mail address turygin@gmail.com/User ID 169389046/Full Name Ivan Turygin ("DROPBOX 3")**
- **Account e-mail address ivan@burfa.com/User ID 996604640/Full Name Ivan Turygin ("DROPBOX 4")**
- **Account e-mail address vadim.tsvetikov@hashcoins.com/Unknown User ID ("DROPBOX 5")**

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

- **Account e-mail address vadim.tsvetikov@burfa.com/User ID 997433824/Full Name Vadim Tsvetikov ("DROPBOX 6")**
- **Account e-mail address vadim@tsvetikov.com/Unknown User ID ("DROPBOX 7")**
- **Account e-mail address tatjana@burfa.com/User ID 2287081056/Full Name Tatjan Potapova ("DROPBOX 8")**
- **Account e-mail address nikolay@hashcoins.com/User ID 997245216/Full Name Nikolay Pavlovskiy ("DROPBOX 9")**
- **Account e-mail address vitali@burfa.com/User ID 731356190/Full Name Vitali Pavlov ("DROPBOX 10")**
- **Account e-mail address anton.altement@polybius.io/User ID 1273000544/Full Name Anton Altement ("DROPBOX 11")**
- **Account e-mail address margarita.burunova@hashcoins.com/User ID 1635854608/Full Name Margarita Burunova ("DROPBOX 12")**

f. **Google LLC** ("Google"), located at 1600 Amphitheater Parkway, Mountain View, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-6, pertaining to the following accounts (collectively the "**GOOGLE ACCOUNTS**"), identified in Attachment A-6:

- **edgar.bers@burfa.com ("GOOGLE 1")**
- **support@hashflare.io ("GOOGLE 2")**
- **altement@gmail.com ("GOOGLE 3")**

4. Upon receipt of the information described in Section I of Attachments B, government-authorized persons will review that information to locate the items described in Section II of Attachments B. This warrant is requested in connection with an on-going investigation in this district by the Seattle Field Office of FBI.

5. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

371 (Conspiracy), 1343 (Wire Fraud), 1956 (Money Laundering), and 1957 (Money Laundering) have been committed by IVAN TURYGIN and SERGEI POTAPENKO, individually, and by and through the use of their companies HASHCOINS OU, HASHCOINS TRADE OU, HASHCOINS LP (collectively, "HASHCOINS"); HASHFLARE LP ("HASHFLARE"); Burfa Capital OU, Burfa Media OU, Burfa Real Estate OU, Burfa Tech OU, Burfa Trade OU, Burfa Invest OU (collectively, the "BURFA Entities"); Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, Polybius Fintech MidCo OU (collectively, "POLYBIUS"); and Dalmeron Projects LP ("DALMERON"), along with other co-conspirators, known and unknown, including identified key employees of the same companies. There is also probable cause to search the information described in Attachments A, for evidence, instrumentalities, or contraband of these crimes, as described in Attachments B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense[s] being investigated." 18 U.S.C. § 2711(3)(A)(i).

7. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

8. This warrant application is to be presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

BACKGROUND ON VIRTUAL CURRENCY AND MINING

9. Virtual currency (also known as cryptocurrency) is an asset that can be exchanged directly person to person, through a virtual currency exchange, or through other intermediaries. It can be used to buy goods and services, exchanged for "fiat currency" (currency established by government regulation or law) or other virtual currency, or held as an investment, among other applications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. Virtual currency is generally not issued by any government or bank. Rather, it is frequently generated and controlled through software operating on a decentralized, peer-to-peer ("P2P") network of computers across the world. (Some types of virtual currency, however, are generated and controlled through software operating on a centralized network of computers across the world.)

11. There are thousands of virtual currencies in use, including Bitcoin, Ethereum, Bitcoin Cash, and Monero. Bitcoin,[1] the most popular form of virtual currency, can be generated through mining. According to Bitcoin.org, "Bitcoin mining is the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins."

12. Bitcoin mining can be conducted locally on a user's computer or other computer hardware, or it can be conducted on another's system via the cloud. According to the Santa Clara Law School High Technology Journal: "Cloud mining is an economic arrangement whereby a person pays another person or entity to engage in cryptocurrency mining on their behalf and receives the transaction fees, cryptocurrency or a portion thereof that is generated from such mining efforts."

13. One measure for determining the effectiveness or processing power of a mining operation is to calculate the operation's hash rate. According to Bitcoin.org: "The hash rate is the measuring unit of the processing power of the Bitcoin network. The Bitcoin network must make intensive mathematical operations for security purposes. When the network reached a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per second."

14. Bitcoin utilizes "public key cryptography," a mathematical algorithm that generates a pair of unique, corresponding keys: the "public key" and the "private key."

---

[1] Since Bitcoin is both a virtual currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the virtual currency. That practice is adopted here.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

These components form the "public address," which is used to send and receive bitcoins and can be shared. A public address is akin to a bank account number, and a private key is akin to a Personal Identification Number ("PIN") or password. Only the holder of a public address's private key can authorize transfers of virtual currency from that public address to another public address.

15. Many virtual currencies operate via a "blockchain," a record (or ledger) of every transaction ever conducted that is distributed throughout the computer network (as opposed to being maintained by any single administrator or entity). As to bitcoins, although the public addresses of those engaging in virtual currency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous.

16. Virtual currency users typically employ a "wallet," a tool that can be used to manage public and private keys, interface with a blockchain, and send or receive virtual currency. Wallets vary widely in terms of their format and technological sophistication. One variety, known as "hosted" (or "custodial") wallets, are virtual-currency wallets controlled by a third party—often, a company with a cloud-based, encrypted wallet platform that may be hosted on the company's servers. Users of hosted wallets may be able to access the company's platform through various digital devices, much like a traditional online banking experience. Hosted wallet providers include virtual currency exchanges, which allow their customers, for a fee, to exchange virtual currency for other virtual currencies and/or fiat currencies.

17. Virtual currencies are sometimes launched through Initial Coin Offerings ("ICO"). An ICO is a capital raising event in which an entity offers investors a unique "coin" or "token" in exchange for consideration—most commonly in the form of established virtual currencies or fiat currency. These tokens are issued on a blockchain and are sometimes

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

listed on online platforms, called virtual currency exchanges, where they are tradable for virtual or fiat currencies. To participate in an ICO, investors are typically required to transfer virtual currencies to the issuer's address, online wallet, or other account. During an ICO, or after its completion, the issuer would typically distribute its unique "tokens" to the participant's unique address on the related virtual currency's blockchain. Similar to stockholders in an initial public offering ("IPO"), holders of tokens are entitled to certain rights related to a venture underlying the ICO, such as profits, shares of assets, use of certain services provided by the issuer, and voting rights.

18. A more detailed description of virtual currencies, blockchains, and law enforcement techniques for investigating virtual currency transactions, is included below.

STATEMENT OF PROBABLE CAUSE

A. Summary of Investigation

19. There is probable cause to believe that Estonian nationals IVAN TURYGIN and SERGEI POTAPENKO, as well as various corporate entities they owned and/or controlled, and other co-conspirators, carried out a multi-faceted wire-fraud and money-laundering conspiracy, in violation of 18 U.S.C. §§ 371, 1343, 1349, 1956, and 1957. As discussed below, from approximately 2014 through 2018, TURYGIN, POTAPENKO, and other co-conspirators deceived and defrauded others in relation to cryptocurrency and cryptocurrency-related ventures, all for their own personal gain. They further engaged in a series of financial and monetary transactions to obfuscate the true nature and location of the fraudulently obtained funds, and to enrich themselves.

20. This fraud scheme had four distinct stages, which together constitute a scheme or artifice to defraud:

a. ***Sale of Cryptocurrency Mining Hardware and Equipment:*** In 2014, through HASHCOINS, TURYGIN and POTAPENKO sold cryptocurrency mining hardware and equipment they did not have. When the influx of contracts to purchase mining equipment far outpaced HASHCOIN's ability to fulfill the contracts, TURYGIN and POTAPENKO revised the contracts to redirect existing and new customers to a purported cloud-based

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

platform to mine Bitcoin and other cryptocurrencies offered by HASHFLARE, which TURYGIN and POTAPENKO also owned and operated.

b. ***Sale of Cryptocurrency Mining Contracts:*** TURYGIN, POTAPENKO, and other co-conspirators operated HASHFLARE as a fraud and Ponzi scheme between in or around 2015 through 2018. During this time, they fraudulently induced thousands of individuals, including one or more of whom resided in the Western District of Washington, to invest in contracts that guaranteed the buyer a portion of HASHFLARE's purported cryptocurrency mining power, and thus a portion of the resulting profits. In order to avoid repaying HASHFLARE investors, TURYGIN and POTAPENKO instituted material changes to the HASHFLARE investor agreements, substantially reducing payments to investors and restricting their abilities to withdraw funds. Then, in July 2018, HASHFLARE unilaterally canceled its contracts with investors and stopped paying annual returns, claiming that cryptocurrency mining was no longer profitable.[2] In fact, the vast majority of annual returns HASHFLARE had paid up to that point were sourced from victims' deposits, not from cryptocurrency mining. To date, the FBI has identified at least $175 million that victims transferred to HASHFLARE, most of which TURYGIN and POTAPENKO laundered through various shell companies, bank accounts, and cryptocurrency wallets they controlled, or otherwise used to perpetuate their fraud scheme.

c. ***Polybius Initial Coin Offering:*** In 2017, leveraging the apparent success of their cloud-mining operations, TURYGIN, POTAPENKO, and others perpetuated their wire-fraud scheme by using proceeds from the initial phase of the scheme—i.e., the HASHFLARE Ponzi scheme—to partially fund the launch of POLYBIUS, and the ICO of PLBT, POLYBIUS's newly minted cryptocurrency token. TURYGIN, POTAPENKO, and others induced victims to purchase tens of millions of dollars of PLBT tokens by making

---

[2] These material alterations and purported cancellation of mining contracts were the subject of a purported class action lawsuit filed in the Central District of California, *Baylog et al. v. Hashflare LP*, No. 18-CV0343. In defending that lawsuit, HASHFLARE continued to falsely represent in court filings that it was a legitimate enterprise and investment vehicle for cloud-based cryptocurrency mining.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

numerous misrepresentations about POLYBIUS and PLBT including, without limitation, that POLYBIUS would use the ICO proceeds to develop a digital bank and would pay dividends to holders of PLBT tokens. Not long after completion of the ICO in June 2017, POLYBIUS publicly dropped any pretext that it intended to build a digital bank. POLYBIUS transferred much of the estimated $32 million it raised in the ICO to shell companies, bank accounts, and/or cryptocurrency wallets controlled by TURYGIN and POTAPENKO.

d. ***Laundering Proceeds:*** TURYGIN, POTAPENKO, and others funneled the fraudulently obtained victim funds through a convoluted network of domestic and international shell companies—including HASHCOINS, DALMERON, and the BURFA Entities—bank accounts, cryptocurrency exchanges, cryptocurrency wallets, and tangible property, all of which they owned and/or controlled, in order to conceal the nature, location, source, ownership, and control of the funds, and to promote additional fraudulent conduct. Additionally, TURYGIN and POTAPENKO used fraud proceeds to fund their lavish lifestyle, which included extensive travel on private jets, stays at luxurious international villas, and the purchase of real estate and luxury cars in Estonia. Even after ostensibly shuttering HASHFLARE, TURYGIN and POTAPENKO used fraud proceeds to purchase expensive cryptocurrency mining hardware, which they used to mine cryptocurrencies for personal gain.

21. The Target Accounts, described in more detail below, are believed to be used to facilitate the scheme and/or associated with the individual or individuals behind the scheme.

B. Procedural History

22. On April 3, 2020, in connection with the pendent investigation, the Honorable Brian A. Tsuchida, United States Magistrate Judge, issued a search warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), requiring Google to disclose to the government copies of certain information and records pertaining to the certain and authorizing the government to seize specified information and records (the "Google Warrant"). *See* MJ20-153. The relevant time period for the information and records

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

subject to disclosure and seizure under the search warrant was the inception of each relevant account through the date of the search warrant.

23. On March 11, 2021, the Honorable John L. Weinberg, United States Magistrate Judge, issued a search warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), requiring Apple Inc. ("Apple") to disclose to the government copies of certain information and records pertaining to certain and authorizing the government to seize specified information and records (the "Apple Warran"). *See* MJ21-149. The relevant time period for the information and records subject to disclosure and seizure under the search warrant was the inception of each relevant account through the date of the search warrant.

24. On April 1, 2022, the Honorable S. Kate Vaughan, United States Magistrate Judge, issued a search warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), requiring Google and Apple to disclose to the government copies of certain information and records pertaining to the previously searched accounts and authorizing the government to seize specified information and records (the "Renewed Warrant"). *See* MJ22-129. The relevant time period for the information and records subject to disclosure and seizure under the search warrant was the date of the previous search warrants through the present.

C. HASHFLARE and HASHCOINS

a. Incorporation and Ownership

25. HASHFLARE and HASHCOINS were incorporated in Estonia and the United Kingdom on the dates listed in the chart below:

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Date	Corporate Name	Country	Legal Form	Directors or Beneficial Owners	Current Name	Prior Names
6/13/13	HASHCOINS OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	Burfa Tech OU	N/A
11/26/14	HASHCOINS TRADE OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	Burfa Trade OU	N/A
12/14/15	HASHFLARE LP	UK	Limited Partnership	Anatoli Sheipak	HASHFLARE LP	Fast Consult Trade LP & HASHCOINS LP

26. HASHFLARE maintained the website hashflare.io, while HASHCOINS maintained the website www.hashcoins.com. According to HASHCOINS' and HASHFLARE's websites, POTAPENKO has been identified as a co-founder and CEO of the entities. According to public reporting, TURYGIN was a co-founder and Business Development Chairman of HASHCOINS. TURYGIN has also been identified as a co-founder of HASHFLARE.

b. Business Operations

27. Beginning in 2014, HASHCOINS advertised the sale of what it deemed to be proprietary cryptocurrency mining hardware. HASHCOINS demanded payment in full up front for all purchases of mining equipment. But by January 2015 at the latest, it became readily apparent that HASHCOINS had sold and continued to sell far more equipment than it had the capacity to build or acquire.

28. Emails obtained by the FBI show that, for most of 2015, HASHCOINS advised its customers of serial delays in the delivery of cryptocurrency mining equipment. Some customers who purchased thousands or tens of thousands of dollars' worth of mining equipment in 2014 still had not received their orders by late 2015 or early 2016. Yet, despite these indefinite delays, HASHCOINS continued to sell mining equipment it did not have and could not build or acquire for much of 2015.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

29. By May 2015, TURYGIN, POTAPENKO, and other co-conspirators set about trying to convert contracts for the purchase and sale of physical cryptocurrency mining equipment through HASHCOINS to the sale of contracts to share in cloud-based cryptocurrency mining revenues through another entity they owned and controlled: HASHFLARE.

30. As a way to stem the flow of customer complaints, HASHCOINS offered to supplement customers with designated hashrates in HASHFLARE's cloud-mining operation, while the customers awaited delivery of the promised merchandise. Emails show that some customers accepted the proposed arrangement, but that HASHCOINS and HASHFLARE failed to deliver the promised hashrate revenues, just as HASHCOINS had failed to deliver the promised equipment.

31. In addition to redirecting existing and new HASHCOINS customers to HASHFLARE, TURYGIN and POTAPENKO began marketing HASHFLARE's purported cloud mining services to the general public on or before April 18, 2015. According to its website, HASHFLARE advertised the following: "Our service makes cryptocurrency mining available to every user. You no longer need to buy expensive equipment and spend your time setting up miners. Just select your desired capacity and earn income!" On another portion of its website, HASHFLARE advertised that "Cloud mining offers a unique option for mining with a low cost of entry as well as minimal risk and expense, which is opposite to traditional models of mining that involve procurement, maintenance and configuration of highly specialized software."

32. In marketing HASHFLARE's cloud-mining services, TURYGIN and POTAPENKO continued to paint HASHCOINS as a legitimate and successful purveyor of cryptocurrency mining hardware, which it was not. HASHFLARE advertised that it conducted its mining in collaboration with HASHCOINS. On its website, HASHFLARE explained that it offered "a new range of cloudmining services brought to you by the HASHCOINS team of cryptomining experts." In turn, on its website, HASHCOINS claimed that it was "an Estonian based cryptocurrency mining hardware manufacturer and cloud

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

hosted mining service provider." HASHCOINS advertised that its users could purchase cloud mining contracts from HASHFLARE, claiming that HASHFLARE users could mine cryptocurrency using HASHCOINS' datacenters. In its terms of service, HASHFLARE stated that "HASHCOINS OU provides technical support, development and marketing of HASHFLARE and its subdomains."

33. HASHFLARE sold cloud mining contracts, purportedly allowing users to mine cryptocurrency through HASHFLARE in exchange for a return. On its website, HASHFLARE explained that a user could "purchas[e] part of the mining power of hardware hosted and owned by a Cloud Mining services provider," which "configur[es] the hardware, maintain[s] uptime and select[s] the most efficient and reliable [mining] pools." For example, on April 18, 2015, for $9.95, a user could buy one million hashrate ("one million hash per second" or "1 MH/s") from HASHFLARE. For this rate, HASHFLARE advertised a "100% Scrypt Miner," automatic accruals in Bitcoin, and a daily maintenance fee of $0.01 per 1/MH/s.

34. HASHFLARE's website advertised a tool that could be used to calculate the approximate amount of profit a user would get depending on the amount of hashrate the user purchased. The user would then have the option to automatically reinvest that profit or withdraw the profit if their balance was above a certain minimum threshold, which fluctuated between 0.05 bitcoin to 0.01 bitcoin throughout the existence and operation of HASHFLARE.

35. In addition to purportedly earning funds through cloud mining, HASHFLARE represented to users that they could earn funds by recruiting others to purchase HASHFLARE contracts. HASHFLARE advertised a referral program, informing users that "as a referrer, you are eligible to receive 10% referral commission bonus for every purchase made by any of your referrals, excluding reinvest and balance purchases." As a result, HASHFLARE users believed they could make money each time one of their referred friends, family members or acquaintances purchased cloud mining contracts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

36. Thousands of individuals, including a number operating in the Western District of Washington, purchased mining contracts from HASHFLARE. According to financial records obtained from Fedwire, a funds transfer system operated by the United States Federal Reserve Banks, at least $2.5 million was transferred to accounts held by HASHCOINS for what appear to be investments in HASHFLARE (examples of descriptions accompanying the transfer of money were: "HASHFLARE.io Invoice…"; "Investments…"; and "…payment for mining services").

37. According to bank records obtained from Latvia, approximately $11 million was transferred into an account held by HASHFLARE at Latvijas Pasta Banka. These transfers were made in the names of various individuals, and often referenced the terms "Invoice" and "Hashrate."

38. Based on the comments included in the financial records obtained by the FBI, as well as my understanding of the HASHFLARE operation as a whole from my review of numerous records and communications, I believe that the payments described in records from Fedwire and Latvijas Pasta Banka were made to purchase cloud mining contracts from HASHFLARE. For example, on January 31, 2017, F.R.E. transferred $1,708 to HASHFLARE's account, referencing "Invoice 593395 Hashflare.io SHA-256 HASHRATE 15." Similarly, on March 6, 2017, A.K. transferred $5,792.72 to HASHFLARE's account, referencing "Invoice .673156 (60TH/S SHA-256 hashrate)."

39. Additionally, according to information obtained from a group of approximately 800 investors, a representative of which contacted law enforcement, between initial investments and re-investments of stated profits, the group collectively invested a total of $7.5 million. It was not readily apparent how much of the $7.5 million was contained within the amounts previously mentioned above.

40. A search of email accounts affiliated with HASHFLARE and HASHCOINS revealed a bank statement, with a date range from January 1, 2017, through September 21, 2018, showing approximately $120 million of deposits into a bank account with the account owner name of "Hashflare LP." The description of most of the deposits was: "Payment from

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

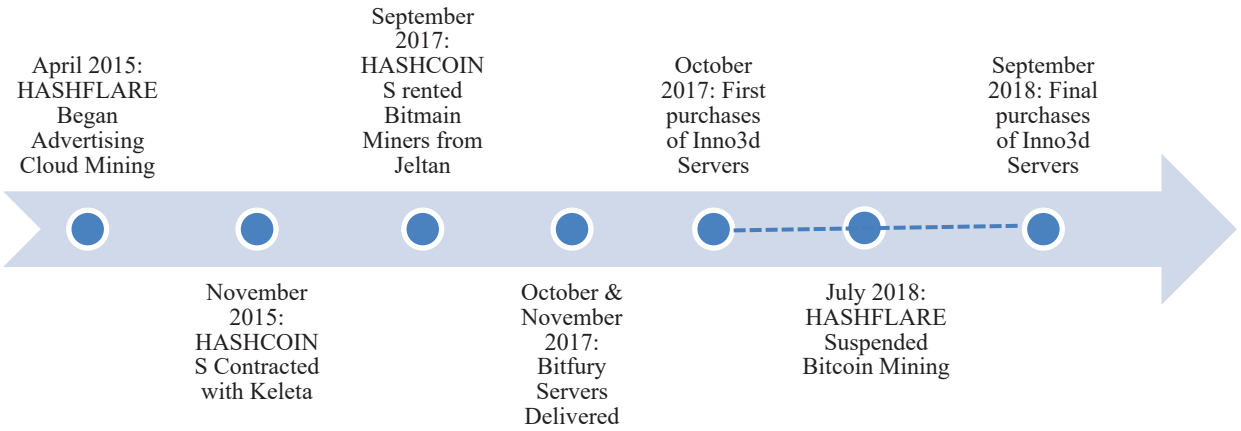
VISA/Mastercard, card processing dd . . . ." A substantial amount of the deposits stopped in or around June of 2018. Based on the same email account review, I know the statements related to a main bank account that received deposits from users of the mining services.

c. HASHFLARE's and HASHCOINS' Cloud Mining Capabilities

41. The FBI has been investigating whether HASHFLARE and HASHCOINS possessed sufficient mining equipment to service the contracts that had been purchased. On its website, HASHFLARE claims that, when the company began in 2015, it conducted cloud mining using equipment obtained from HASHCOINS. As referenced above, investors questioned whether HASHCOINS had the capability to mine cryptocurrency, since the entity did not appear to have a large server location.

42. Additionally, in 2014, HASHCOINS initially sold mining equipment, to be operated by the purchasing user. However, during that time frame, HASHCOINS claimed that it experienced supply disruptions, frustrating its ability to supply Bitcoin mining equipment. As a result, HASHCOINS offered its customers the opportunity to invest in HASHFLARE's cloud-mining services, instead. Investors questioned whether HASHCOINS had the ability to produce cloud mining equipment.

43. Law enforcement has reviewed various financial records, along with email records, to determine what cloud mining resources were purchased by HASHFLARE. Based on these records, it appears that, at various times, HASHCOINS or HASHFLARE contracted with Keleta UAB, Bitmain, Bitfury, and Inno3d vendors to provide cloud mining services. These services at described below and depicted in the following visual chart:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

44. In 2015, it appears that HASHCOINS entered into a Mining Hardware Rent Agreement with a Lithuanian company named Keleta UAB. Specifically, on October 31, 2015, HASHCOINS entered into a contract with Keleta UAB for the purpose of renting SHA-256 Protocol cryptocurrency mining hardware. Pursuant to the terms of this contract, over the course of one year, HASHCOINS obtained € 600,000 worth of hashrate. The service was set to start on November 1, 2015. A further search of the email accounts provided a HASHCOINS bank statement, with a date range of January 1, 2015, through February 24, 2017, showing that HASHCOINS transferred € 575,000 to Keleta UAB. Attached to certain emails were six invoices, issued from Keleta UAB to HASHCOINS, which totaled € 575,000.

45. Of note, there is no publicly available information regarding Keleta UAB that confirms that this company actually provides mining hardware. According to public databases, the address listed on the cryptocurrency mining contract for Keleta UAB also serves as the registered address for numerous other Lithuanian companies. Based on my training and experience, and information gained during the course of this investigation, I know that incorporation companies often register multiple companies, including shell companies, using the same business address.

46. In 2017, HASHFLARE and HASHCOINS entered into contracts with Bitmain, Bitfury, and Inno3d cloud mining vendors. This is consistent with HASHFLARE's website, where beginning on or before June 4, 2018, HASHFLARE advertised, albeit in broken English, that it uses "equipment for mining" obtained from "Bitmain, Bitfury, Inno3d, and others." Bitmain, Bitfury, and Inno3d each manufacture cryptocurrency mining equipment. Because of the broken English, it is difficult to determine when HASHFLARE started using

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

mining equipment supplied by these companies, but it appears that HASHFLARE advertised that it acquired this equipment in 2016.[3]

47. While law enforcement has not identified evidence that HASHFLARE purchased mining equipment in 2016, it has located evidence that a limited amount of funds was transferred to these vendors in 2017, during the final months of HASHCOINS' and HASHFLARE's operations.

48. *First*, according to an email sent to TURYGIN, on September 1, 2017, HASHCOINS entered into a contract with a UK company named Jeltan Trading LP for the purpose of renting Bitmain Antminer L3+ hardware. Pursuant to the terms of this contract, HASHCOINS purchased $1,000,000 worth of hashrate over the course of a year. According to bank records HASHCOINS transferred € 918,000 to Jeltan Trading LP between September 19, 2017, and November 13, 2017.

49. Of note, there is no publicly available information regarding Jeltan Trading LP that confirms that this company actually owns or rents mining hardware. According to public databases, the address listed on the cryptocurrency mining contract for Jeltan Trading LP also serves as the registered address for numerous other UK companies. Based on my training and experience, and information gained during the course of this investigation, I know that incorporation companies often register multiple companies, including shell companies, using the same business address.

50. *Second*, according to information obtained from Bitfury, on August 3, 2017, Bitfury entered into an agreement to sell HASHCOINS ten "Bitfury B8 server[s] with proprietary BitFury hardware (16 nm) capable of producing up to 43 TH/s (±5%) of SHA 256 hashing power ('Hashing Power') and consuming 6.4 KW (±5%) of electricity" for $52,000. Additionally, on September 25, 2017, Bitfury entered into an agreement to sell

---

[3] The language states: "HashFlare is a cloud mining service created by the specialists from HashCoins in 2015. In a short time, HashFlare became one of the largest providers of computational power for mining bitcoin, litecoin, ethereum and other cryptocurrencies. From 2016, HashFlare is an independent company. The variety of equipment that is used for mining was significantly increased on the account such companies as Bitmain, Bitfury, Inno3d and others."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

HASHCOINS 154 "Bitfury Europe configured B8 server[s] with proprietary Bitfury hardware (16 nm) capable of producing up to 43 TH/s (±5%) of SHA 256 hashing power ('Hashing Power') and consuming 6.4 KW (±5%) of electricity." In exchange for these servers, HASHCOINS paid Bitfury $926,772.[4] Records from Bitfury show that deliveries of these servers were made on October 16, 2017, and November 21, 2017; however, e-mail communications show that the servers were not installed until January or February of 2018.

51. Furthermore, on October 12, 2017, TURYGIN and a HASHCOINS representative exchanged emails with a Bitfury representative, discussing a "4M order next week right after 1M." The HASHCOINS representative explained that "the 4M order is . . . not yet confirmed." Based on the context of this email, I believe 4M to refer to $4,000,000. I have seen no evidence suggesting that this $4 million purchase was completed. Rather, according to banking records obtained to date,[5] HASHCOINS first transferred funds, in the amount of $52,000, to Bitfury on August 14, 2017, with another transfer of funds, in the amount of $926,772, occurring on October 4, 2017. These funds transfers were consistent with the amounts identified in the above-mentioned contracts.

52. *Third*, bank statements for both HASHCOINS and Burfa Media show that, between October of 2017 and September of 2018, approximately $13 million was transferred to ASK Technology, which sells Inno3d-branded products. A search of email accounts belonging to Burfa Media personnel contained a summary of 23 invoices totaling approximately €16 million due to ASK Technology Group Limited. Based on the discrepancy between payments made to ASK Technology and the invoice totals that were compiled by Burfa Media, the amount of product purchased from ASK Technology was unclear.

---

[4] Bitfury also entered into subsequent agreements, in 2018, to sell equipment to HASHCOINS' successor, BURFA MEDIA OU.

[5] The FBI is continuing to gather financial information related to this case and has, so far, obtained records from Latvia, Estonia, and the United States relating to HASHFLARE and HASHCOINS, among other entities.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

53. In addition to Bitfury, Bitmain, and Inno3d, law enforcement has identified evidence suggesting that payments were made to other cryptocurrency mining providers.

54. For example, in January 2018, HASHCOINS transferred € 79,415.87 to BDC Mining EHF. According to publicly available information, BDC Mining EHF is based in Iceland.

55. Additionally, HASHFLARE transferred funds to DALMERON for "SHA-256" and "According to a Computational Power Rent Agreement from 16.02.2018." According to documents located in email accounts used by HASHFLARE and HASHCOINS personnel, Anatoli Sheipak serves as the "ultimate beneficial owner" of DALMERON. However, for the following reasons, it appears that the owners of HASHFLARE and HASHCOINS—TURYGIN and POTAPENKO—are the true beneficial owners of DALMERON. First, on July 26, 2017, TURYGIN emailed an incorporation company, requesting that a related company, Dalmeron Invest, be incorporated, listing Anatoli Sheipak as the director and owner of the entity. Additionally, on October 26, 2017, GoDaddy sent POTAPENKO an email recommending that he renew the domain registration for dalmeron.com. Anatoli Sheipak was also listed as the sole subscriber for HASHFLARE's Microsoft account, suggesting that he is affiliated with HASHFLARE. And, finally, TURYGIN's email account, turygin@gmail.com, is linked by cookies to dalmeronprojects@gmail.com. Accordingly, based on my training and experience, and information gained during the course of this investigation, I believe that DALMERON is a subsidiary or is otherwise associated with HASHFLARE and HASHCOINS, rather than an independent company providing cloud mining services.

56. As described above, HASHCOINS and HASHFLARE began purchasing or renting cryptocurrency mining equipment from third parties in November 2015, with the bulk of their purchases occurring in the final months of their operations (September 2017 through June 2018), as well as after HASHFLARE ceased operations (July 2018 through September 2018). Based on financial records analyzed to date, users appeared to have begun transferring funds to HASHCOINS' bank accounts to purchase HASHFLARE mining

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

contracts in or before November 2015. For example, on November 29, 2015, a transfer was made to an account held by HASHCOINS TRADE OU with the accompanying description: "Invoice #32789 ivanovdmi3i@list.ru HashFlare.io SHA-256 hashrate 300GH/s." These transfers were made before any known delivery of mining equipment was made by these vendors to HASHFLARE or HASHCOINS. Based on the above, the FBI is investigating whether HASHFLARE was soliciting and collecting investments for services it was not yet able to sufficiently perform.

57. Additionally, since neither Jeltan Trading LP nor Keleta UAB have any appreciable public presence online, the FBI is also investigating whether those entities are legitimate, providing actual services to HASHFLARE or HASHCOINS.

58. Between at least August 2017 and June 2018, HASHFLARE also transferred more than € 25 million to CryptoPay Ltd., a UK company that sells Bitcoin, purchases Bitcoin in exchange for fiat currency, and sells cards that can be loaded with cryptocurrency. For example, on August 8, 2017, HASHFLARE transferred $250,000 to CryptoPay Ltd. for "digital assets purchase." Again, on August 17, 2017, HASHFLARE transferred an additional $250,000 for "digital assets purchase." These payments continued through at least June 7, 2018, when HASHFLARE transferred $800,000, also for "digital assets purchase." Based on these purchases, and the payment references, the FBI is investigating whether HASHFLARE was paying its investors using bitcoins purchased from CryptoPay, rather than mining bitcoins as advertised.

d. Law Enforcement's Review of HASHFLARE's and HASHCOINS' Activity on the Blockchain

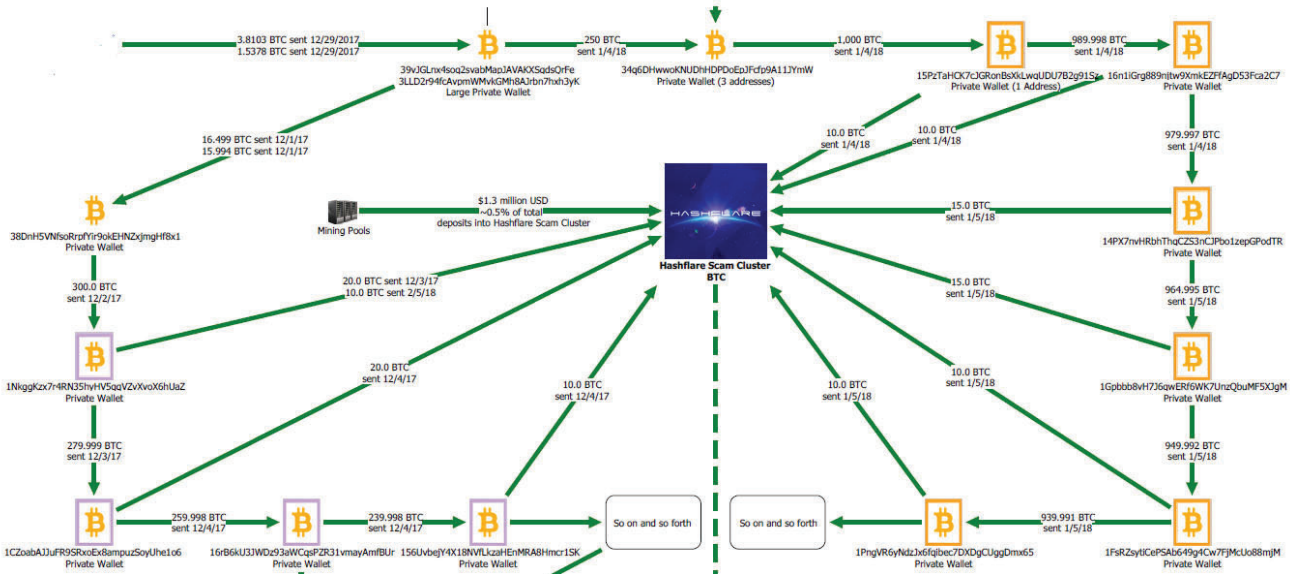
59. In addition to obtaining evidence that HASHFLARE and HASHCOINS did not maintain anywhere close to the level of cloud mining to service the contracts sold by the two companies to the public, law enforcement—including the FBI—analyzed HASHFLARE's and HASHCOINS' activity on the blockchain, as well as those of the companies' beneficial owners, TURYGIN and POTAPENKO, to assess the source of purported mining revenue payments made to customers. Such analyses revealed that the vast majority of payments

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

made to customers derived from a pool of victim deposits, which TURYGIN, POTAPENKO, and others funneled through a series of hosted and private cryptocurrency wallets designed to make it appear as though victims who received payments were actually sharing in mining revenues, as opposed to simply receiving a portion of newer victims' deposits.

60. For example, POTAPENKO used a personal wallet hosted by Bittrex, Inc., a cryptocurrency exchange headquartered in Seattle, Washington, to convert bitcoin—purchased from Cryptopay using victims' fiat funds deposited with HASHFLARE—into ether, which POTAPENKO then deposited in a HASHFLARE wallet used to repay victims.

61. TURYGIN and POTAPENKO employed a "peel chain"—a technique often used to launder large amounts of cryptocurrency by using a lengthy "chain" of smaller transactions. In a peel chain, a small portion of the overall amount to be transferred "peels" off from the main address in a relatively low-value transfer. (In this case, TURYGIN and POTAPENKO would "peel" off chunks of 10 to 20 bitcoin for transfer into a larger HASHFLARE scam cluster.) The remaining balance of the larger cryptocurrency amount—the "change"—transfers to a new change address, and the process repeats itself until the desired larger transfer is complete. A visual depiction of the peel chain is set forth below:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

62. TURYGIN and POTAPENKO's use of a peel chain here appears designed to prevent or disrupt victims from tracing payments they received from HASHFLARE back to the wallets that had received the initial victim deposits.

63. From 2015 through 2020—more than a year after HASHFLARE shuttered its operations in July 2018—the FBI estimates that HASHFLARE received approximately $175 million in deposits from customers purchasing contracts to share in HASHFLARE's cryptocurrency mining operations. During that same time period, the FBI estimates that HASHFLARE generated $2.2 to $3.4 million from mining cryptocurrencies. Accordingly, the vast majority of the funds HASHFLARE had available to pay victims' annual returns derived from victim deposits, not from cryptocurrency cloud-mining operations.

64. Estonian authorities independently analyzed HASHFLARE's cryptocurrency transactions, including 22,935 transfer chains related to HASHFLARE payout wallets, to determine if payouts to investors were coming from mining pools, which would be the expected source of payouts. They reached similar conclusions as those reached by the FBI. Based on their analyses, Estonian authorities concluded that most of the payouts to victims came from the wallets where Bitcoin deposits were received, and only 0.8% of payouts came from mining pools.

65. Based on the foregoing analyses, among others, it appears that HASHFLARE was not engaged in substantial cryptocurrency mining, as previously advertised. Instead, as described above, HASHFLARE appears to have operated as a Ponzi scheme by converting victims' deposits from fiat to cryptocurrency, or from one cryptocurrency to another, in order to pay back other victims and to conceal the true source of those payments.

e. Collapse of HASHFLARE's Ponzi Scheme

66. Starting in or around August of 2017, HASHFLARE made a number of changes to its operations. For example, HASHFLARE changed its terms of service that shortened the length of exiting Bitcoin mining contracts from "lifetime" contracts to "one year" contracts. Functionally speaking, under lifetime contracts purchased hashrates did not

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

expire, whereas under the new term the purchased hashrates expired after one year, requiring users to buy additional contracts.

67. In or around July 2018, HASHFLARE also required all users to submit "Know Your Customer" identification before they could continue using services offered on the platform. In effect, these additional procedures reduced the ability of users to withdraw funds earned through mining. On online forums, users complained that, even after they submitted the necessary documentation, HASHFLARE was taking weeks or months to verify their identities and pay balances. Other users complained that they never received their requested balances.

68. Finally, on July 20, 2018, HASHFLARE announced that Bitcoin mining had been unprofitable for 28 days as of July 18, 2018, and that, per clause 5.5 of its Terms of Service, all Bitcoin mining SHA-256 contracts were suspended. According to its terms of service, HASHFLARE informed investors that it would stop cryptocurrency mining "if the Maintenance and Electricity Fees [are] larger than the Payout." Specifically, according to HASHFLARE's terms, "If mining remains unprofitable for 21 consecutive days the Service is permanently terminated . . . [and] Payouts and Fees will also be temporarily stopped."

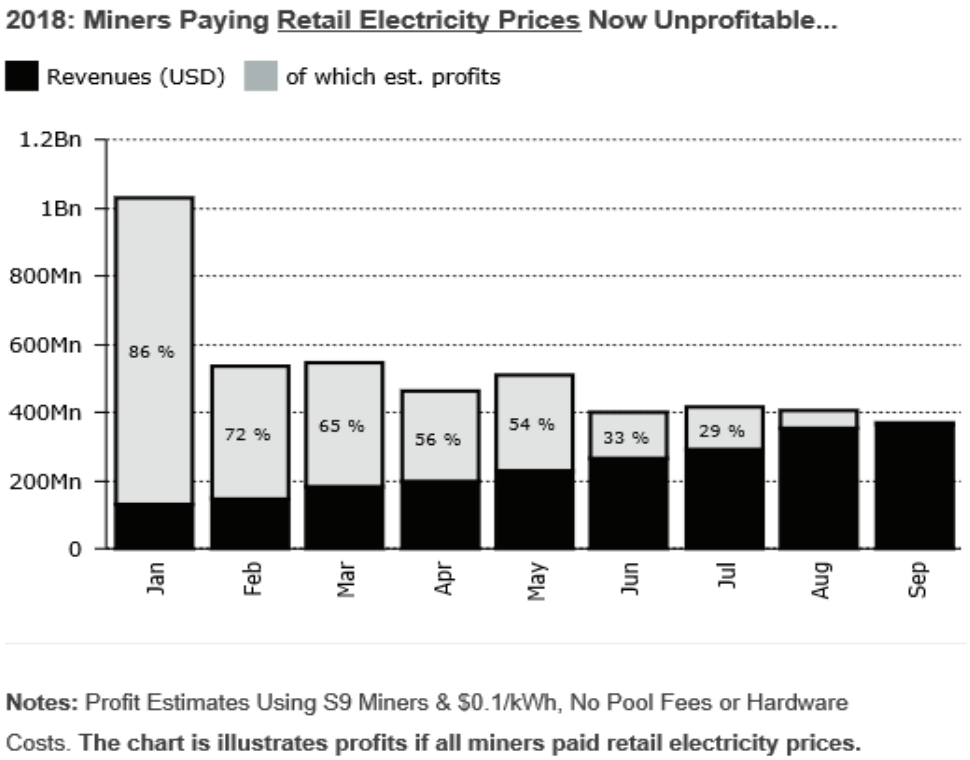
69. Interviews of three HASHFLARE investors, F.M., B.J., and F.W., revealed that it was not possible to make any withdrawals once the Bitcoin mining contracts were suspended, which held true through the dates of the interviews that took place in or around September of 2019. Since then, there has been no indication from known victims that any of the money invested was recoverable from HASHFLARE.

70. Since HASHFLARE suspended its contracts, investors, including those located in the United States, began identifying red flags which led them to believe that HASHFLARE was a Ponzi scheme that was not engaged in cryptocurrency mining. Instead, they believed that HASHFLARE was profiting on fluctuations in cryptocurrency exchange rates, using those gains and new investment proceeds to repay earlier investors. For example, investors visited HASHFLARE's business address in Estonia, which did not appear to house a server farm or computing equipment consistent with cryptocurrency mining.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Additionally, according to these investors, the rates charged by HASHFLARE for maintenance and electricity were above market average, and pools that were used to mine did not produce the expected output.

71. Diar, which publishes a digital assets and regulations newsletter, reported that while bitcoin mining was profitable for the first six months of 2018, with 2018 revenues exceeding 2017 revenues by $1.4 billion, as of the end of August and the beginning of September, bitcoin mining was becoming unprofitable.[6] According to Diar, increases in electricity costs and mining difficulty (increased hashrate) have led to this unprofitability. For example, a chart compiled by Dial is referenced below:



72. While Diar projected that mining did not become unprofitable until late August and early September 2018, HASHFLARE contended that its mining operations became

[6] Diar, *Bitcoin Miner Revenues Near $5 Billion but Profitability Dwindles*, Volume 2, Issue 40, (Oct. 8, 2018), *available at* https://diar.co/volume-2-issue-40/.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

unprofitable in late June 2018. However, HASHFLARE's operations may be more costly than those profiled by Diar, which did not take pool fees or hardware costs into account. HASHFLARE's terms of service provide that users must pay the following maintenance fees: "hardware setup, data center rent, Mining Pool testing, staff salaries, future planning and proofing, software development, exchange of used and out of order parts and other expenditures required to render the service on a best-effort basis."

73. Although HASHFLARE claimed a sudden drop in cryptocurrency mining profitability forced it to cease operations, HASHFLARE appears to have only engaged in nominal cryptocurrency mining activities during the relevant time periods. Instead, HASHFLARE—at the direction of TURYGIN and POTAPENKO—appears to have operated as a Ponzi scheme, as described above, by converting victims' deposits from fiat to cryptocurrency, or from one cryptocurrency to another, in order to pay back other victims.

74. Furthermore, based on my training and experience, and information gained during the course of this investigation, I know that Ponzi schemes operate by recruiting others, paying earlier investors with funds transferred by later investors. Ponzi schemes often involve recruitment bonuses, incentivizing earlier investors to recruit friends and family members so that funds are available to pay earlier members. As described above, HASHFLARE advertised a referral program, paying earlier investors 10% bonuses based on cloud mining contracts purchased by those they referred.

75. HASHFLARE and HASHCOINS have stopped selling any mining contracts and, as described below, its founders and employees appear to have moved to successor companies that continue to operate in the cryptocurrency space. Prior investors have not been able to recoup their funds and many have been unable to transfer funds held in their accounts.

76. On December 29, 2020, an Estonian news company "DV" published an article describing a police investigation of POTAPENKO and TURYGIN. The article provided, in part, that POTAPENKO and TURYGIN were being investigated for fraud that was facilitated through HASHFLARE's purported cloud-mining operations.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

77. As part of this article, TURYGIN wrote to DV asserting that a Scottish firm, Fast Consult LP, bought the HASHFLARE cloud-mining operations in March 2016. According to TURYGIN, Fast Consult LP renamed itself to HASHCOINS LP, and later HASHFLARE. TURYGIN explained that HASHCOINS, a company he and POTAPENKO own, but which was distinguishable from HASHCOINS LP, which TURYGIN and POTAPENKO did not own, provided IT services and technical support to HASHFLARE for two years after its sale.

78. On December 31, 2020, TURYGIN published his own article in DV in response to the December 29, 2020, article, further claiming that HASHCOINS TRADE OU assisted HASHCOINS LP with accepting funds until the fall of 2016, but after that HASHCOINS LP began to independently accept its own funds into their own accounts.

79. TURYGIN's assertions are not supported by the evidence gathered to date in this investigation. For example, an E-shop Agreement for payment card acceptance was signed by TURYGIN on or around May 24, 2017, which named IVAN TUROGIN as the authorized representative of HASHCOINS LP. According to the terms of the agreement, reports would be sent to the email address sergei@hashcoins.com, associated with POTAPENKO. The E-shop Agreement also provided that, while the legal address for HASHCOINS LP was listed as 44/46 Morningside Road, Suite 3, Edinburgh, EH10 4BF, Scotland, United Kingdom, the actual address provided was Tartu Mnt 43, 10128 Estonia – the address utilized by the BURFA Entities, HASHCOINS, and Polybius, as well as TURYGIN's own Apple registration address. Furthermore, in an email dated January 30, 2017, POTAPENKO explained to the representative of a payment processing company that HASHCOINS LP operates in Estonia and not the United Kingdom.

80. I submit there is probable cause to believe HASHFLARE and HASHCOINS operated as a Ponzi scheme for at least the following reasons: (1) before its collapse, HASHFLARE appears to have been in financial distress, as evidenced by its unilateral conversion of mining contracts from lifetime contracts to year-long contracts, its use of KYC requirements to delay users' withdrawal of funds from their accounts, and its termination of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

mining contracts during a time when industry press considered bitcoin mining to be profitable; (2) HASHCOINS' questionable ability to manufacture cryptocurrency mining equipment, as evidenced by its 2014 decision to not fulfill equipment orders and instead convert purchase contracts to HASHFLARE cloud mining contracts; (3) Estonian law enforcement's analysis that HASHFLARE was not receiving substantial payouts from mining pools, sufficient to pay its investors; (4) HASHFLARE's apparent purchase of "digital assets" from CryptoPay, which, among other items, sells Bitcoin, suggesting that HASHFLARE may have purchased cryptocurrency rather than mined it; (5) HASHFLARE's inherent structure, including its referral program and lack of transparency regarding its mining pools, which is a common structure evidenced in Ponzi schemes; (6) TURYGIN's public attempt to mask true ownership of the now-defunct cloud-mining company; and (7) as described in further detail below, HASHFLARE's dissolution and the subsequent transition of its employees and co-founders, who joined new companies that continue to operate in the cryptocurrency space.

D. Other Linked Entities

a. BURFA Entities

81. After HASHFLARE terminated its mining contracts, HASHCOINS OU changed its legal name to Burfa Tech OU and HASHCOINS TRADE OU changed its name to Burfa Trade OU. As described below, a number of HASHCOINS and HASHFLARE employees then transferred and started working for these entities.

82. Burfa Tech OU and Burfa Trade OU are part of a conglomerate formed by TURYGIN and POTAPENKO, under the umbrella company Burfa Capital OU, incorporated in Estonia (collectively called the "BURFA Entities"). These entities are described below:

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Date	Corporate Name	Country	Legal Form	Directors or Beneficial Owners	Prior Names
7/12/13	Burfa Capital OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	Starfix UU
6/27/13	Burfa Media OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	N/A
7/17/17	Burfa Real Estate OU	Estonia	Private Limited Company	Pavel Ivanov	Burfa Estate OU
6/13/13	Burfa Tech OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	HASHCOINS OU, Euro Host UU
11/26/14	Burfa Trade OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	HASHCOINS Trade OU, Habalink UU
6/27/13	Burfa Invest OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	N/A

83. According to the website for Burfa Capital, burfa.com, the various entities have the following missions:

a. Burfa Capital OU "is a commercial organization . . . emphasizing collaboration and investment in such priority areas as IT, fintech and data processing." Burfa Capital OU appears to be the parent corporation in the BURFA Entities conglomerate.

b. Burfa Media OU "provides computing equipment for processing large data arrays and for any operations that require significant computing power."

c. Burfa Real Estate OU "is engaged in the construction of commercial and residential luxury real estate in Estonia . . . for the subsequent sale or rent."

d. Burfa Tech OU is reported to be "a leader in the field of data center design and maintenance for the industrial sector . . . specializ[ing] in high-performance computing and turnkey data center solutions." Like HASHCOINS, Burfa Tech OU is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

reported publicly to be "an IT company operating in Estonia mainly in the field of equipment for cryptocurrency mining."

e. Burfa Trade OU and Burfa Invest OU have been removed from their website.

84. As described in the chart below, a number of the individuals employed by the BURFA Entities, or who at one time were employed by the BURFA Entities, appear to have been formerly employed by HASHCOINS or HASHFLARE.

Name	Role in HASHCOINS or HASHFLARE	Role in BURFA Entities
SERGEI POTAPENKO	Co-Founder and CEO of HASHFLARE and HASHCOINS	Board Member & Co-Founder of Burfa Capital OU
IVAN TURYGIN	Co-founder of HASHFLARE and HASHCOINS	Board Member & Co-Founder of Burfa Capital OU
Nikolay Pavlovskiy	Chief Technology Officer of HASHCOINS, Vice President and Head of Business Development at HASHFLARE	Chief Technology Officer for Burfa Capital OU
Vitali Pavlov	Project Manager at HASHFLARE, Chief Product Officer at HASHCOINS	Chief Product Officer at Burfa Capital OU
Vadim Tsvetikov	Data Center Operation Director at HASHCOINS	Data Center Operation Director for Burfa Capital OU
Pavel Tsihhotski	Support and Community Manager for HASHCOINS	Head of Support for Burfa Capital OU
Stanislav Pavlov	Associated with HASHCOINS	Human Resources Manager and Customer Support for Burfa Tech OU
Tatjana Potapova	Chief Financial Officer for HASHCOINS	Chief Financial Officer for Burfa Media OU
Edgar Bers	Public Relations Business Development Manager for HASHCOINS	Associated with BURFA Entities—possesses @burfa.com email address

85. Additionally, around the time the Bitcoin mining contracts were suspended, HASHFLARE transferred substantial assets to the BURFA Entities. For example, according

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

to bank records gathered during the course of this investigation, two different bank accounts held in the name of HASHFLARE transferred approximately $15.5 million to a bank account in the name of Burfa Media OU throughout the year in 2018.

86. The @burfa.com domain was established on August 22, 2017, listing two contact email addresses—admin@burfa.com and sergei@hashcoins.com (associated with POTAPENKO).

b. POLYBIUS

87. In addition to HASHCOINS, HASHFLARE, and the BURFA Entities, TURYGIN and POTAPENKO have also formed another conglomerate, comprised of four entities—Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, and Polybius Fintech MidCo OU (collectively, referred to as "POLYBIUS").

88. Each of these entities was incorporated in Estonia, as listed below:

Date	Corporate Name	Country	Legal Form	Directors or Beneficial Owners
2/13/17	Polybius Foundation SE	Estonia	European Company	TURYGIN, POTAPENKO & Anton Altement
2/1/18	Polybius Tech OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO, Anton Altement & Dmitri Ahmarov
2/8/18	Polybius Ventures OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO & Anton Altement
4/25/18	Polybius Fintech MidCo OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO, Anton Altement & Mathieu Hardy

89. According to the website for POLYBIUS, Polybius.io, and public reporting, the various entities have the following missions:

a. Polybius Tech OU created a cryptocurrency wallet called OSOM Finance, designed to hold both Bitcoin and alternative coins.

b. Polybius Ventures OU and Polybius Fintech MidCo OU are not separately described but are both subsidiaries in the POLYBIUS ecosystem.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. Polybius Foundation, according to its Prospectus and Whitepaper—two published documents that purported to explain the structure and purpose of the ICO, POLYBIUS was, at the time of the ICO, "a team of financial, security, legal and technical experts" who intended to raise funds to start Polybius Bank. The alleged intent was for Polybius Bank to be a "fully digital bank accessible everywhere at any time." POLYBIUS further represented that the digital bank "will have all the functions of a classical bank, but will not host any branches, nor any physical front-offices and will rely fully on the latest digital technologies." The front of the prospectus reads, in part: "Polybius POWERED BY HASHCOINS."

90. The FBI analyzed numerous financial records relating to the operations of HASHCOINS, HASHFLARE, the BURFA Entities, DALMERON, and POLYBIUS. Based on its analyses, the FBI concluded that TURYGIN and POTAPENKO used the foregoing companies they owned and/or controlled to indirectly transfer more than $5 million from HASHFLARE to POLYBIUS between January 2015 and February 2019.

91. According to an article written by Forbes on October 29, 2018, POLYBIUS raised approximately $32 million dollars during its ICO in the summer of 2017. The symbol for the POLYBIUS token is PLBT.

92. In connection with the ICO, TURYGIN, POTAPENKO, and others, by and through POLYBIUS, made a number of representations, which now appear to be false. They touted the apparent successes of HASHFLARE and HASHCOINS, which they actually operated as a fraud and Ponzi scheme. They claimed that POLYBIUS would use the funds it raised in the ICO to develop a "fully digital bank" described in its prospectus and whitepaper. They claimed to have partnered with various established institutions, including the accounting and consulting firm EY, in order to bolster their credibility and legitimacy. And they claimed the resulting POLYBIUS bank or payment institution would pay 20 percent of its distributable profits as annual dividends to holders of PLBT tokens.

93. Estonian authorities have opined that the PBLT ICO likely violated Estonian law for several reasons, including that POLYBIUS should have known at the time it

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

advertised the ICO that it could not obtain an Estonian banking license using funds obtained from an anonymous crowdsourcing event.

94. Moreover, as of the date of the Forbes article referenced above, no tangible product had been launched. In fact, POLYBIUS announced that it abandoned the prospect of opening a bank, and that it would develop a mobile application instead. It is unclear whether the mobile application would qualify as a bank or payment institution such that PLBT holders would be entitled to share in the application's distributable profits.

95. A cursory review of the POLYBIUS tokens was discussed in a law review article published by the Columbia Law Review in April of 2019, entitled "Coin-Operated Capitalism." In the article, the authors note that a "development team can unilaterally change the [POLYBIUS] tokens purchased by investors—or sometimes, propose changes that will not be adopted if a certain percentage of users do not object." The authors opine that the latter type of proposed changes that may be detrimental to investors may automatically take effect with no knowledge of the investor because (1) the default vote is inherently set to "yes," and (2) the investing public as a whole does not have the technical skills to monitor or understand the proposed changes a development team may make to the POLYBIUS tokens. To date, it is unknown whether any such changes occurred.

96. On November 17, 2018, POLYBIUS released a blog post announcing it was releasing a new personal finance management service called "OSOM." Later in 2019, POLYBIUS released instructions about how to transfer PLBT tokens from an investor's POLYBIUS Wallet to their OSOM Wallet. According to POLYBIUS, transfer of the PLBT tokens to the OSOM Wallet was important because the POLYBIUS Wallet would eventually no longer be functioning.

97. The POLYBIUS coin is still available for trading as of today, and both the OSOM website and POLYBIUS websites promote the OSOM product.

98. OSOM's website lists four products it offers: a) Crypto Autopilot, a cryptocurrency portfolio managed by artificial intelligence; b) DeFi Earn, a cryptocurrency

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

lending platform; c) Insights, a cryptocurrency news and data hub; and d) Gift, a way to buy Bitcoin and gift it to people.

99. There is no mention of plans to establish a bank on either the POLYBIUS or OSOM websites.

100. As with the BURFA Entities, some of the individuals who are, or were, employed by POLYBIUS appear to have been formerly employed by HASHCOINS or HASHFLARE or the BURFA entities. As a result, it appears that POLYBIUS is a successor entity of HASHCOINS and HASHFLARE. The chart below compares individuals' roles in HASHCOINS, HASHFLARE, or BURFA with their roles in POLYBIUS:

Name	Role in HASHCOINS, HASHFLARE or BURFA	Role in POLYBIUS
SERGEI POTAPENKO	Co-Founder and CEO of HASHFLARE and HASHCOINS	Co-Founder of POLYBIUS
IVAN TURYGIN	Co-founder of HASHFLARE and HASHCOINS	Co-Founder of POLYBIUS
Edgar Bers	Public Relations Business Development Manager for HASHCOINS	Product Manager for OSOM
Pavel Tsihhotski	Support and Community Manager for HASHCOINS	Associated with POLYBIUS (possessed @polybius.io email address)
Anton Altement	Associated with BURFA Entities (possesses @burfa.com email address)	CEO & Co-Founder of POLYBIUS
Vitali Pavlov	Project Manager at HASHFLARE, Chief Product Officer at HASHCOINS	Product Manager POLYBIUS

101. Moreover, the FBI's financial and blockchain analyses show that POLYBIUS has received millions of dollars of funds and cryptocurrency from accounts and wallets held in the names of other entities owned or controlled by TURYGIN and POTAPENKO, including the BURFA Entities and DALMERON. POLYBIUS also appears to have sent millions of dollars of cryptocurrency to wallets controlled by the BURFA Entities and POTAPENKO.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

E. Summary of the ACCOUNTS

102. In the paragraphs below, I provide additional information about the various ACCOUNTS. For the reasons set forth herein, there is probable cause to believe that the Accounts contain evidence relevant to this criminal investigation and will assist investigators to 1) determine false statements that were made to the public to induce them to invest in HASHFLARE or POLYBIUS, 2) identify additional victims who made contact with representatives of HASHFLARE or POLYBIUS, 3) determine documents and other records that were developed to facilitate laundering of the Ponzi scheme proceeds, 4) further investigate the mining capabilities of HASHFLARE and the other companies affiliated with its purported cloud-mining service, and 5) further investigate the underlying business plan and strategy of the ICO that was advertised to be for funding POLYBIUS Bank.

103. As discussed below, based on my training and experience and that of other trained investigators, I know that electronic service providers, such as Twitter, Facebook, Slack, ZenDesk, and Dropbox, offer a variety of services and generally maintain extensive records related to customers and service users, including, but not limited to, direct communication between the service user and a member of the public, posts made by service users for the public to view (such as advertisements or marketing materials), and the person(s) in control of the TARGET ACCOUNTS.

I. Twitter ACCOUNTS

104. **Username "turygin" ("TWITTER 1"):** According to records provided by Twitter, the Twitter account for username "turygin", ID 176428871 (TWITTER 1), was created on August 9, 2010, using IP address 90.191.76.75, and is associated with email turygin@gmail.com. Records provided by Google show that TURYGIN created the e-mail address turygin@gmail.com

105. I have searched for public postings made by TWITTER 1, and discovered the account appears to currently be suspended. Based on my training and experience, and my review of Twitter terms of service, I know that Twitter account suspensions can be temporary or permanent, Twitter may retain possession of data and content related to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

suspended accounts, and Twitter users may in some cases be able to reinstate or unsuspend suspended accounts.[7]

106. Twitter's terms of service include a ban on ICOs; a restriction on advertising cryptocurrency exchanges, cryptocurrency hot wallets, cryptocurrency ATMS, cryptocurrency credit and debit cards; and the need for prior approval from Twitter for advertising other types of cryptocurrency products or services. Since TURYGIN, the owner of TWITTER 1, was a founder of a company that launched an ICO, and the founder of a company that allegedly cloud-mined cryptocurrency, it is possible that TWITTER 1 was banned for violating Twitter's terms of service.

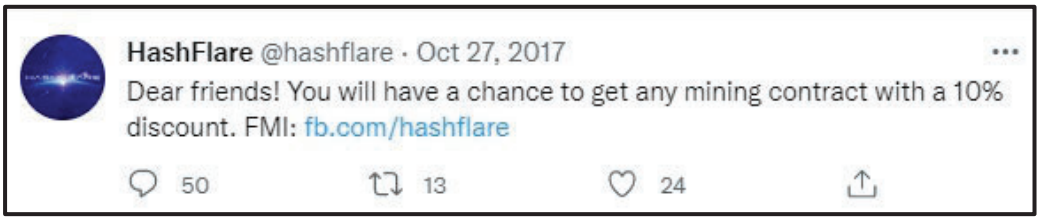
107. **Username "hashflare" ("TWITTER 2"):** I searched Twitter for the profile of TWITTER 2, which shows that it was established in December 2014, its location is Tallinn, Estonia, and the description of the profile is "Cloudmining service":

[7] *See, e.g.,* https://help.twitter.com/en/managing-your-account/suspended-twitter-accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

108. I reviewed the public postings made by TWITTER 2 and discovered multiple posts promoting the HASHFLARE cloud-mining service throughout its existence. In 2016, TWITTER 2 posted the following advertisement to entice the public to buy contracts for the HASHFLARE cloud-mining service:

Similar public postings were made in 2017 and 2018, offering discounts on cloud-mining contracts to further attract the public to make purchases:

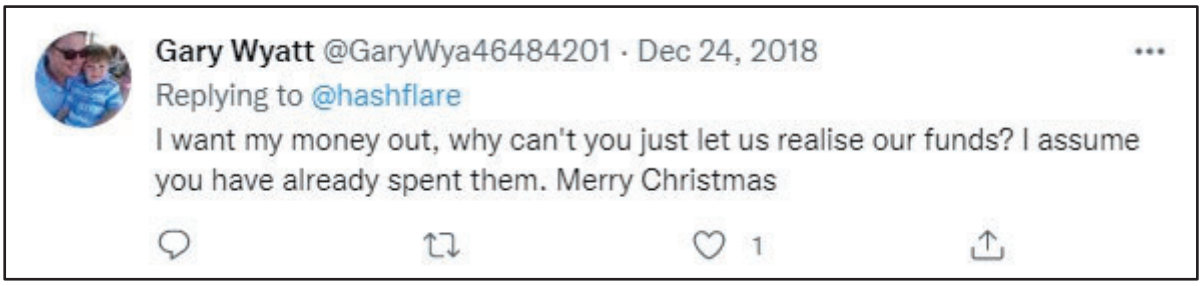


109. After HASHFLARE shut down its SHA-256 mining operations on July 24, 2018, it announced on July 27, 2018, that operations would resume on July 28, 2018. However, I learned from interviews and conducting research in the public domain that HASHFLARE cloud-mining contract-holders were still unable to make withdrawals from

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

their account, and in some instances, they could not even access their accounts. TWITTER 2 made a public post on December 24, 2018, wishing its users a Merry Christmas:

110. The Merry Christmas posting garnered many replies, most of which were people asking for their money back or calling HASHFLARE scammers, an example of which is as follows:



111. Aside from promoting HASHFLARE, TWITTER 2 also promoted the POLYBIUS Initial Coin Offering:

//

//

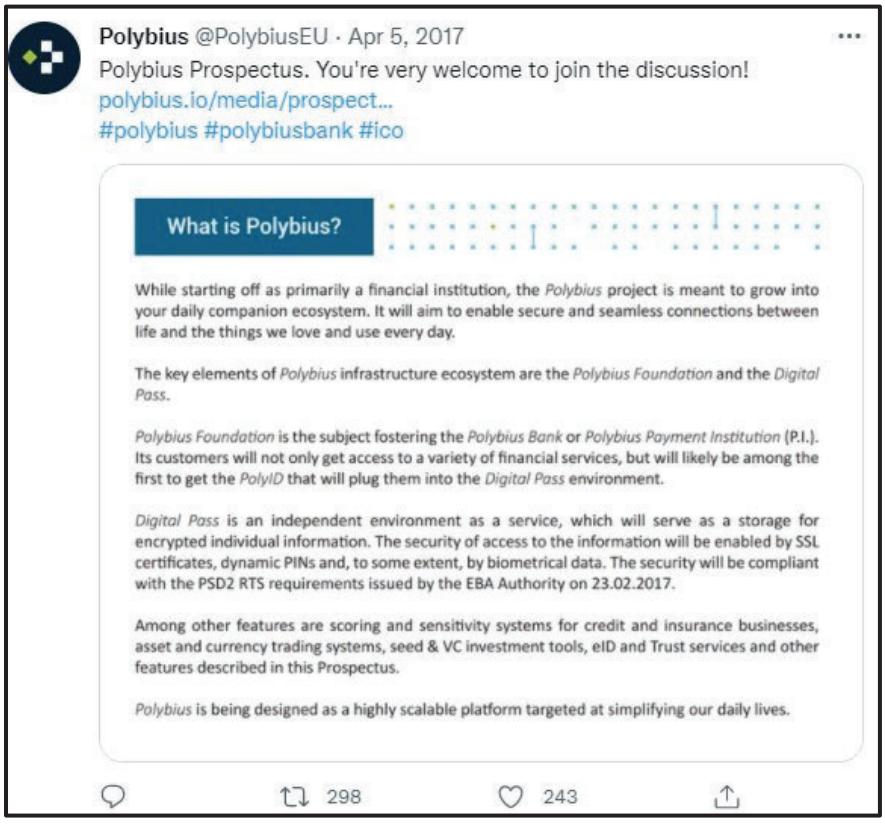
//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

112. **Username "PolybiusEU" (TWITTER 3):** I searched Twitter for the profile of TWITTER 3, which shows that it was established in December 2016, its location is Estonia, and contains a link to Polybius.io:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

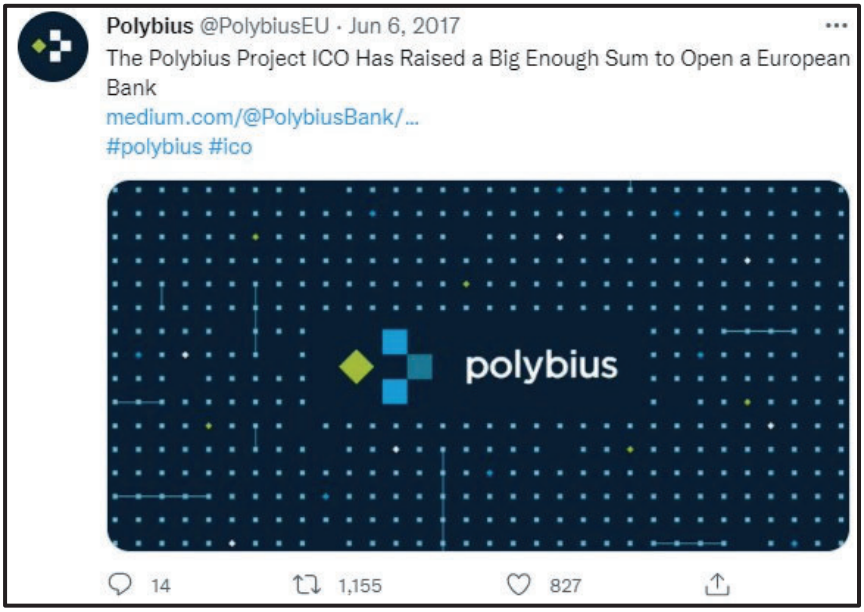
113. I reviewed public postings made by TWITTER 3, one of which was a Prospectus which discusses, in part, the creation of POLYBIUS Bank:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

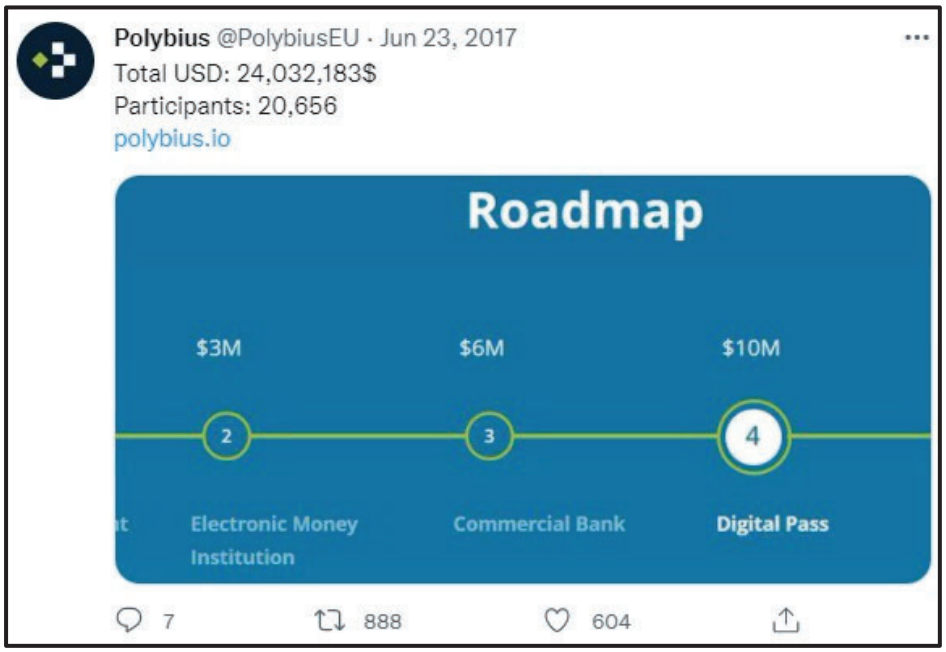
114. On May 30, 2017, TWITTER 3 announced the launch of ICO crowd funding for a digital bank project – POLYBIUS:

115. Throughout the POLYBIUS ICO, which spanned from May 31, 2017, through June 29, 2017, TWITTER 3 continued to promote the ICO and the POLYBIUS Bank, including a public post from June 6, 2017, providing that the ICO raised enough to open a European bank:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

116. And a public posting on June 23, 2017, providing the ICO raised over $24 million, and a progress chart showing that POLYBIUS exceeded the amount of capital needed to open a commercial bank:



117. I believe that TWITTER 3 continuously posted about the success of the ICO, and its ability to establish a bank, to continue to attract additional investment from the public.

118. Over two years later, on September 6, 2019, POLYBIUS published a posting on Polybius.io acknowledging that it had yet to release a product and that it was not currently pursuing the creation of a bank, which was continuously promoted as a main goal of the ICO.

119. Based on a review of the Polybius.io website on March 11, 2022, there is a roadmap providing a list of goals for POLYBIUS in 2021, none of which include establishing a bank. The POLYBIUS website does currently appear to be maintained, mostly providing updates about OSOM Finance.

120. Based on the above, I believe that TWITTER 1, 2, and 3 were used for the purpose of promoting and perpetuating fraudulent activity. As such, I believe probable cause exists to conclude the accounts contain evidence pertinent to the investigation, including 1)

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

communication with victims, and 2) false statements made to the public to attract investment.

II. Meta ACCOUNTS

121. The investigation has uncovered at least one HASHFLARE Facebook account that is associated with the Ponzi scheme, and two other Facebook accounts that I have probable cause to believe are associated with the Ponzi scheme.

122. **Vanity Name HashFlareGlobal ("FACEBOOK 1"):** I searched Facebook for the profile of FACEBOOK 1 and found a profile with the display name "HashFlare Cloud Solutions", with an "About" section describing that HASHFLARE is a remote computer processing power rent service, providing the Twitter handle "@hashflare", and a website located at "hashflare.io".

123. The second post on FACEBOOK 1, published on April 4, 2018, acknowledged that HashFlare's original Facebook page was unpublished because it violated Facebook's terms of service. However, the content that was published on FACEBOOK 1 contained similar advertisements that were found on TWITTER 2, such as discounts on cloud-mining contracts to entice the public to make purchases from HASHFLARE. An example of which was posted on April 4, 2018, advertising a 30 percent discount:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

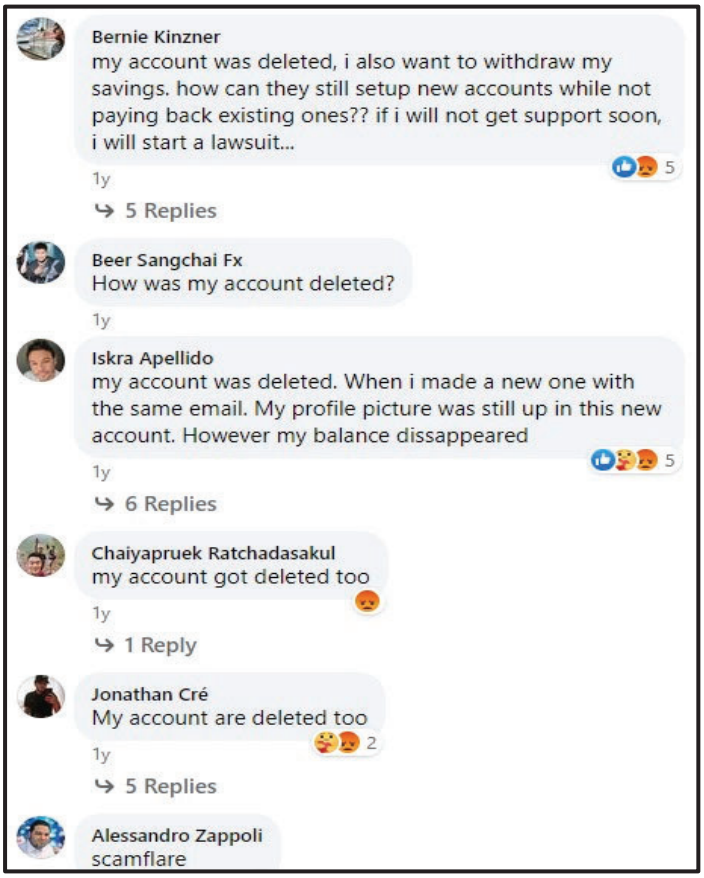
124. And later, on May 22, 2018, a post was made advertising a 22% discount on contracts:

125. FACEBOOK 1 posted similar content as TWITTER 2 regarding the shutdown of HASHFLARE's SHA-256 mining operations on July 24, 2018, and eventually announced on July 27, 2018, that SHA-256 mining would resume on July 28, 2018. However, I learned from interviews and conducting research in the public domain that HASHFLARE cloud-mining contract-holders were still unable to make withdrawals from their account, and in some instances they could not even access their accounts.

126. The last post made by FACEBOOK 1 was on August 8, 2019, providing that HASHFLARE was suspending sale of ETHASH contracts, and acknowledging it was not mining ETHASH and SHA-256.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

127. In response to this post, there were numerous complaints, some of which acknowledged that their accounts with HASHFLARE were unilaterally deleted:



128. **Vanity Name "turygin" (FACEBOOK 2):** According to records provided by Facebook, the Facebook account for vanity name "turygin", ID 100002183784122 (FACEBOOK 2), was registered on March 15, 2011, and is associated with e-mail address turygin@gmail.com.

129. Records provided by Google associate the e-mail address "turygin@gmail.com" with TURYGIN.

130. I searched Facebook for public postings of FACEBOOK 2 and discovered that the account appears to be a private account and, as such, I cannot view any of the activity taking place in the account.

131. However, FACEBOOK 1, the public account of HASHFLARE, a company founded and operated by TURYGIN, was used to advertise HASHFLARE. Based on my

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

training and experience I believe that since TURYGIN had the propensity to advertise HASHFLARE on its public Facebook profile, there is probable cause to believe that he similarly used his own Facebook account, FACEBOOK 2, to advertise HASHFLARE.

132. **Vanity Name "sergei.pt" (FACEBOOK 3):** According to records provided by Facebook, the Facebook account for vanity name "sergei.pt", ID 1764433774 (FACEBOOK 3), was registered on April 26, 2009, and is associated with e-mail address "sergei.potapenko@gmail.com".

133. Records provided by Google associate the e-mail address "sergei.potapenko@gmail.com" with SERGEI POTAPENKO.

134. I searched Facebook for public postings of FACEBOOK 3. I discovered that the account appears to be a private account and, as such, I cannot view any of the activity taking place in the account.

135. However, FACEBOOK 1, the public account of HASHFLARE, a company founded and operated by POTAPENKO, was used to advertise HASHFLARE. Based on my training and experience I believe that, since POTAPENKO had the propensity to advertise HASHFLARE on its public Facebook profile, there is probable cause to believe that he similarly used his own Facebook account, FACEBOOK 3, to advertise HASHFLARE.

136. Based on the above, I believe that FACEBOOK 1, 2, and 3 were used for the purpose of promoting and perpetuating fraudulent activity. As such, I believe probable cause exists to conclude the accounts contain evidence pertinent to the investigation, including 1) communication with victims, and 2) false statements made to the public to attract investment.

III. Slack ACCOUNTS

137. The investigation has uncovered numerous instances where Slack was referenced by both POLYBIUS and HASHCOINS personnel as a communication facility. In addition, a 2703(d) Order served to Slack provided records showing that there were

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

numerous Slack Workspaces[8] created for both POLYBIUS and HASHCOINS.

138. **Workspace name "BDC" ("SLACK 1"):** According to records provided by Slack, the workspace "borealisdc.slack.com" (SLACK 1) was created on March 12, 2015.

139. I reviewed the user logs for SLACK 1 and observed that multiple users with HASHCOINS e-mail addresses were members, including: vitali@hashcoins.com, simin.inkin@hashcoins.com, and mihkel@hashcoins.com.

140. During my investigation I found an e-mail sent on or around March 29, 2018, by Vitali Pavlov, who was the Chief Product Officer of HASHCOINS, using the e-mail address vitali@hashcoins.com, to send an e-mail to representatives of Borealis Data Center in Iceland, where I know HASHCOINS had cryptocurrency miners installed. The e-mail asked for updates to be communicated via Slack. I know that the workspace's name, "BDC", stands for "Borealis Data Center".

141. **Workspace name "HashCoins" ("SLACK 2"):** According to records provided by Slack, the workspace "hashcoins.slack.com" (SLACK 2) was created on October 1, 2015.

142. I reviewed the user logs for SLACK 2 and observed that at least two users with HASHCOINS e-mail addresses were members: vitali@hashcoins.com and simin.inkin@hashcoins.com; a user with a HASHFLARE e-mail address was a member: renna@hashflare.io; and the former Chief Technology Officer of HASHCOINS, Nikolay Pavlovskiy was also a member, using what appears to be a personal e-mail address.

143. **Workspace name "Polybius" ("SLACK 3"):** According to records provided by Slack, the workspace "polybiusbank.slack.com" (SLACK 3) was created on December 7, 2016.

144. I reviewed the user logs for SLACK 3 and observed that the "Primary Owner" of the workspace used the e-mail address "info@polybius.io" and the name "Polybius

[8] According to slack.com, a "Slack workspace is made up of channels where team members can communicate and work together."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Team"; an "Admin" user of the workspace used the e-mail address "support@polybius.io" and the name "Polybius Bank"; and another "Admin" user of the workspace used the e-mail address "vitali@hashcoins.com" and the name Vitali Pavlov, who was known to be the Product Manager for both HASHCOINS and POLYBIUS.

145. During my investigation I uncovered an e-mail sent on or around May 3, 2017, by the e-mail address "info@polybius.io", which used the name "Polybius Bank". The e-mail was sent to a person, "K.M.", who appeared to be inquiring about the timing of the Polybius ICO. The response by POLYBIUS Bank is provided below, which includes a reference to joining POLYBIUS on Slack:

Re: when will ico start?

From: Polybius Bank <info@polybius.io>
To: [redacted]
Date: Wed, 03 May 2017 01:05:16 -0700

Hi, [redacted]

Thank you for your message and showing such interest in our business!

The exact launch date of the ICO hasn't been finalized yet. Meanwhile, subscribe to our newsletter or join us on social media to get all the latest news.

Telegram: http://t.me/polybius_eng

Bitcointalk: https://bitcointalk.org/index.php?topic=1848751.msg18395912#msg18395912

Twitter: https://twitter.com/PolybiusBank

Facebook: https://www.facebook.com/polybiusbank/

Slack: https://polybius.io/#contacts

Blog: https://medium.com/@PolybiusBank

Best regards,

Pavel

Polybius.io team

146. **Workspace name "Polybius" ("SLACK 4"):** According to records provided by Slack, the workspace "polybius-io.slack.com" (SLACK 4) was created on August 22, 2018.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

147. I reviewed the user logs for SLACK 4 and observed that an "Admin" user of the workspace was Anton Altement, the CEO and co-founder of POLYBIUS; a user of the workspace was Edgar Bers, a product manager for POLYBIUS; and a guest of the workspace was TURYGIN, also a co-founder of POLYBIUS.

148. During my investigation, I uncovered an e-mail sent on or around March 27, 2019, by Dmitri Gerassimov, the Financial Controller of Polybius Tech OU, to Anton Altement. In the e-mail, Gerassimov writes to Altement, in part, that he can answer questions by e-mail or Slack messages.

149. Accordingly, based on my training and experience, as well as the above information, I believe that members of POLYBIUS and HASHCOINS utilized Slack to discuss internal operations of the companies and to communicate with the public. As such, I believe probable cause exists to conclude that SLACK 1, 2, 3, and 4 contain evidence pertinent to the investigation, such as 1) the true operational status of the companies, 2) what the employees planned to represent to the public, and 3) what was actually presented to the public.

IV. Zendesk ACCOUNTS

150. **Account Name hashflare ("ZENDESK ACCOUNT"):** Zendesk provides a service that facilitates communication between companies and their customers. I reviewed an invoice submitted by Zendesk to HASHFLARE, and it appears that HASHFLARE created a ZENDESK ACCOUNT beginning on or around November 25, 2015.

151. Through the course of my investigation, I have read several requests for support submitted by customers of HASHFLARE. The following text was contained at the bottom of each request for support: "This email is a service from HASHFLARE Support. Delivered by Zendesk". The answers to the requests for support appear to originate from a common e-mail address: "support@hashflare.io".

152. On December 17, 2015, a HASHFLARE user put in a request for support because their hash rate "disappeared without explanation". That communication was then sent to "sergei@hashcoins.com", an e-mail address known to be used by POTAPENKO:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

[HashFlare Support] Re: t1: withdrawal

From: [redacted] (HashFlare Support) <support@hashflare.io>
To: HashFlare Support <sergei@hashcoins.com>
Date: Thu, 17 Dec 2015 07:09:02 -0800

##- Please type your reply above this line -##

This ticket (#41587) has been updated.

[redacted]

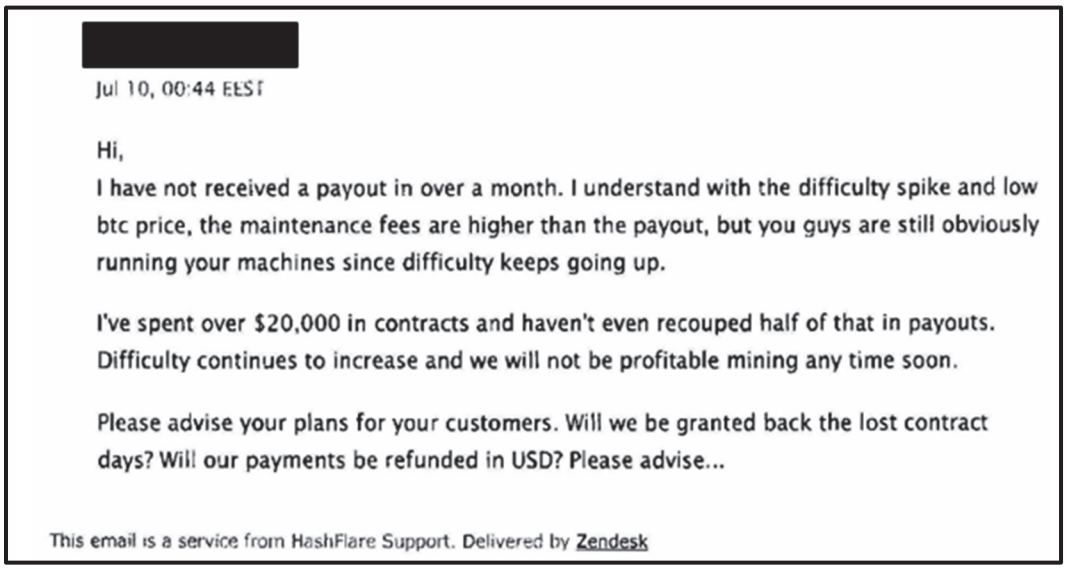
Dec 17, 17:09

Hi,

Thank you. But suddenly all our hash rate disappeared without explanation.
Both the 7.5TH SHA256 and 250MH Scrypt.
While I though we agreed on continuing the review package and getting to update it once X11 would be available.
If not resolved, it means from this point forward we stop updating the review.
But hopefully it doesn't come to this.

Kind regards,

153. On July 10, 2018, a HashFlare user put in a request for support because they stopped receiving payouts:



[redacted]

Jul 10, 00:44 EEST

Hi,
I have not received a payout in over a month. I understand with the difficulty spike and low btc price, the maintenance fees are higher than the payout, but you guys are still obviously running your machines since difficulty keeps going up.

I've spent over $20,000 in contracts and haven't even recouped half of that in payouts. Difficulty continues to increase and we will not be profitable mining any time soon.

Please advise your plans for your customers. Will we be granted back the lost contract days? Will our payments be refunded in USD? Please advise...

This email is a service from HashFlare Support. Delivered by Zendesk

154. Based on the above, I believe the ZENDESK ACCOUNT was used for the purpose of promoting and perpetuating fraudulent activity. As such, I believe probable cause

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

exists to conclude the accounts contain evidence pertinent to the investigation, including communication with victims.

V. Dropbox ACCOUNTS

155. Throughout the course of my investigation, I have received records from Dropbox in response to a grand jury subpoena. The records show that multiple persons affiliated with HASHFLARE, HASHCOINS, BURFA, and POLYBIUS had registered accounts with Dropbox, including POTAPENKO, TURYGIN, Nikolay Pavlovskiy, Tatjana Potapova, Anton Altement, Vitali Pavlov, Vadim Tsvetikov, and Margarita Burunova – collectively identified as the DROPBOX ACCOUNTS.

156. In addition to the registered DROPBOX ACCOUNTS, I also discovered during my investigation that Dropbox was used to exchange documents among and between HASHFLARE, HASHCOINS, BURFA, and POLYBIUS personnel.

157. For instance, on or around January 30, 2017, POTAPENKO, using the e-mail address "sergei@hashcoins.com", references Dropbox when communicating with a representative from UniversePay, a payment processor located in Latvia. I know that UniversePay was used to accept credit card payments for purchasing HASHFLARE'S cloud mining contracts. POTAPENKO referenced Dropbox in response to the UniversePay representative's inquiry about providing a contract to confirm that HASHCOINS rents server power from DALMERON, and to provide a contract between HashCoins LP and HashCoins OU.[9] I believe that POTAPENKO provided the contracts to the UniversePay representative via Dropbox.

158. Based on my training and experience, I know that the aforementioned type of documentation is typically collected as part of anti-money laundering due diligence. I believe that UniversePay was requesting contracts proving that HASHFLARE/HASHCOINS was engaged in mining in order to confirm they had legitimate operations.

---

[9] The original version of the referenced e-mail was composed in the Russian Language. An English version was created using a language translation software, which is how I was able to read it.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

159. Also, on or around April 3, 2018, POTAPENKO used Dropbox to send TURYGIN's e-mail address, "turygin@gmail.com", a link to a Dropbox folder entitled "HashFlare.io". The Dropbox account used by POTAPENKO to send TURYGIN the Dropbox link was linked to "sergei.potapenko@gmail.com".

160. Additionally, on or around September 26, 2018, Potapova, using e-mail address, "tatjana@burfa.com", sent an e-mail to Julia Karpa, an employee at BURFA, instructing her to upload numerous documents into a Dropbox folder, the descriptions of which included: HashCoins, Burfa Capital, Dalmeron Projects, and Burfa Media[10].

161. Based on the above, I believe the DROPBOX ACCOUNTS were used for the purpose of promoting and perpetuating fraudulent activity. As such, there is probable cause to believe that information contained in the DROPBOX ACCOUNTS could reveal, among other things: 1) the plans and strategies formed by the users of the DROPBOX Accounts to defraud investors and customers, 2) the actions taken to execute those plans, 3) the operations and relationship between the various entities, 4) the extent and capacity of mining operations at HASHCOINS and HASHFLARE; and 5) documents that were created to assist with laundering the Ponzi scheme proceeds.

VI. Google ACCOUNTS

162. During this investigation, I obtained records from Google, pursuant to the Google Warrant, relating to Google accounts associated with emails used by various individuals and entities believed to be involved in the wire-fraud and money-laundering conspiracies described in this affidavit. Google 1 was originally included among the Google accounts identified to be searched in the Google Warrant; however, a clerical error resulted in the misspelling of "edgar.bers@burfa.com" as "edger.bers@burfa.com", and the account was not searched. The FBI had not identified Google 2 or Google 3 at the time of the Google Warrant application, so those accounts were not included among the Google accounts searched at that time.

[10] *Id.*

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

163. According to information obtained from Google, the BURFA Entities use the email domain @burfa.com, which is hosted by Google. The billing address for this domain is Burfa Media OU, in the care of SERGEI POTAPENKO. Burfa Media OU uses G Suite, a Google product that provides cloud computing, productivity, and collaboration tools for business clients.

164. The @burfa.com domain was established on August 22, 2017, listing two contact email addresses—admin@burfa.com and sergei@hashcoins.com (associated with POTAPENKO). As of December 2019, the Burfa entities used the Google services Google Calendar, Google Drive, Google Docs, Gmail, Google+, Google Hangouts, Groups for Business, Hangouts Chat, Jamboard Service, Keep, Sites, and Tasks.

165. As of December 2019, there were 42 email addresses associated with the domain @burfa.com. Among those identified as most relevant to this investigation is **edgar.bers@burfa.com, GOOGLE 1**, which is used by Edgar Bers. Bers is responsible for product development for the BURFA Entities.

166. Additionally, as discussed in paragraphs 149–153, customers who made requests to HASHFLARE for support—including requests related to customers' apparent inability to withdraw funds from their accounts—received responses from **support@hashflare.io**, **GOOGLE 2**.

167. As described above, Anton Altement the CEO & Co-Founder of POLYBIUS. He is also associated with the BURFA Entities and possesses an @burfa.com email address. Through this investigation, I have also learned that Altement has on occasion used the email address **altement@gmail.com**, **Google 3**, to communicate with some of the other email addresses included in and searched pursuant to the Google Warrant.

168. Based on the above, I believe the GOOGLE ACCOUNTS were used for the purpose of promoting and perpetuating fraudulent and money laundering activities. As such, there is probable cause to believe that information contained in the GOOGLE ACCOUNTS could reveal, among other things: (1) the plans and strategies formed by the users of the GOOGLE ACCOUNTS to defraud investors and customers, (2) the actions taken to execute

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

those plans, (3) the operations and relationship between the various entities, including assets transferred between those entities; (4) communications with victims; and (5) the location of assets paid by investors to HASHCOINS, HASHFLARE, and/or POLYBIUS.

BACKGROUND CONCERNING META

169. Meta owns and operates Facebook, a free-access social networking website that can be accessed at http://www.facebook.com. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

170. Meta asks Facebook users to provide basic contact and personal identifying information either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

171. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

172. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

173. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

174. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can "tag" other users in a photo or video, and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

175. Facebook users can use Facebook Messenger to communicate with other users via text, voice, video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats. of the date of each call. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

176. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

177. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

178. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

179. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

180. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

181. In addition to the applications described above, Meta provides users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

182. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user's IP address is retained by Meta along with a timestamp.

183. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables "Location History," "checks-in" to an event, or tags a post with a location.

184. Social networking providers like Meta typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

185. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

186. Therefore, the servers of Meta are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

BACKGROUND CONCERNING TWITTER[11]

187. Twitter owns and operates a social networking and microblogging service of the same name that can be accessed at http://www.twitter.com and via the Twitter mobile application ("app"). Generally, Twitter allows users to register and create an account; to personalize (if desired) an account profile page; and to send and receive communications via the platform. These functionalities are discussed in more detail below.

188. Twitter permits its users to communicate via messages that can contain photos, videos, links, and/or a maximum of 280 characters of text. Users can choose to share these messages, called "Tweets," with the public or, alternatively, to "protect" their Tweets by making them viewable by only a preapproved list of "followers." Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Users can also Tweet a copy of other Tweets ("retweet") or Tweet a reply to another Tweet. Users can also indicate that they like a Tweet by clicking on a heart icon that appears next to each Tweet on the platform.

189. Twitter also permits its users to exchange private messages, known as "direct messages" or "DMs," with other Twitter users. DMs, which also may include photos, videos, links, and/or text, can only be viewed by the sender and designated recipient(s). Direct messages may be sent to an individual user or to a group of up to 50 Twitter users.

---

[11] The information in this section is based on information published by Twitter on its website, including, but not limited to, the following document and webpages: "Guidelines for law enforcement," available at https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support, "Using Twitter," available at https://help.twitter.com/en/using-twitter, and "New user FAQ," available at https://help.twitter.com/en/new-user-faq.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Twitter users have the ability to choose whether they can receive a direct message from anyone. At any time, a Twitter user has the ability to alter the settings on their Twitter account so that they can receive direct messages only from (1) individuals to whom the user has already sent a direct message and (2) Twitter accounts that the user "follows" via his account.

190. While individuals are not required to register with Twitter to view the content of unprotected Tweets, individuals must register for a Twitter account to send Tweets, to "follow" accounts in order to view protected Tweets, and to send and receive direct messages. A user may register for an account for free by visiting Twitter's website or via the Twitter app. When a user creates a new Twitter account, Twitter assigns that account a unique user ID ("UID"). A user must also select a password as well as a unique Twitter username (also known as a "handle"). Twitter then appends the @ symbol in front of whatever username the user selects to create the Twitter username (for example: @example). The user may also select a different name (the "display name"), which is not automatically preceded by the @ symbol, to be displayed on his profile picture and at the top of his Tweets alongside his Twitter username. The display name can include symbols similar to emojis. The user can change their password, username, and/or display name at any time, but the UID for the account will remain constant.

191. While anyone can sign up and use Twitter for free, as of November 2021 Twitter also offered a subscription model that offered users access to additional features and app customizations. This new subscription is called Twitter Blue. A user can sign up for Twitter Blue at any time.

192. At the time of account creation, Twitter asks the user for certain identity and contact information, including: (1) name; (2) email address and/or telephone number; and (3) month and year of birth. Twitter also keeps certain information relating to the creation of each Twitter account, including: (1) the date and time at which the user's account was created; and (2) the method of account creation (e.g., website or Twitter app).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

193. Upon the creation of a Twitter account, a generic profile page is automatically created for the user. This page displays information including (1) the user's Twitter username; (2) the display name; (3) the number of Twitter accounts the user is following; (4) the number of Twitter accounts that are following the user; and (5) Tweets sent by the user (although, as noted above, if the user has chosen to protect their Tweets they will be visible only to preapproved "followers"). The user can personalize this page by posting a personal picture or image (known as an "avatar") to appear on the page and/or a banner image to appear across the top of the profile page. The user can also add text to create a short biography, to identify his location, to provide a link to his website, or to specify his date of birth.

194. As noted above, Twitter users can use their account to send and receive communications. If a Tweet includes a Twitter username that is preceded by the @ symbol, that is referred to as a "mention." The Twitter user mentioned in the Tweet will receive a notification informing them that they have been mentioned and showing the content of that Tweet. Similarly, if another Twitter user replies to a Tweet sent by a user, the user who sent the original Tweet will receive a notification that someone replied to their message, and the notification will show the content of that reply.

195. Twitter users can also include links to webpages in their Tweets and Direct Messages. Twitter automatically processes and shortens links provided by the user to a shortened link that starts http://t.co/. Twitter tracks how many times these shortened links are clicked.

196. A registered Twitter user can also "like" a Tweet by clicking a heart icon on a Tweet sent by another user. If another user "likes" a Tweet that is posted by the Twitter user, a notification will appear in the user's account identifying what Tweet was liked and who liked it.

197. As noted above, users can include photographs, images, and videos in their Tweets. Each account has a "media timeline" on their profile that displays "the photos,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

videos, and GIF's [the accountholder] has uploaded with [their] Tweets." An individual can view a Twitter user's media timeline by visiting the user's Twitter profile page.

198. Twitter users can also opt to Tweet with their location attached. This functionality is turned off by default, so Twitter users must opt-in to utilize it. However, if a Twitter user enables Twitter to access their precise location information, the Twitter user will have the option of attaching their location (e.g., the name of a city or neighborhood) to a Tweet at the time it is sent. If the user uses Twitter's in-app camera to attach a photo or video to the Tweet while the functionality is enabled, the Tweet will include both the location label (e.g., the name of a city or neighborhood) of the user's choice as well as the device's precise location in the form of latitude-longitude coordinates. The user can turn this functionality off (thereby removing their location from their Tweets) at any time, and they can delete their past location data from Tweets that have already been sent.

199. A Twitter user may choose to "follow" another Twitter user. If a Twitter account is unprotected (i.e., privacy settings have not been enabled), the user can follow another user simply by clicking the "follow" button on the other user's Twitter profile page. If a Twitter account is protected (i.e., privacy settings have been enabled), the user can follow another user by clicking the "follow" button and waiting for the other user to approve their request. Once an account is followed by a Twitter user, the Tweets posted by the account the user follows will appear in the user's Twitter Home timeline. Every time a Twitter user follows another account, Twitter sends a notification to the account being followed to inform them about the new follower. Each user's Twitter profile page includes a list of the people who are following that user and a list of people whom that user follows. Twitter users can "unfollow" other users whom they previously followed at any time. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting based on the types of accounts that the user is already following and who those people follow.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

200. A Twitter user can also "block" other Twitter users. This prevents the blocked account from contacting or following the user or from seeing the user's Tweets. Twitter does not notify the user of a blocked account when another Twitter account blocks them.

201. A Twitter user can also use Twitter's integrated search function. When a user types a search term into Twitter's search tool, it will return results that include accounts, Tweets, and photos that match that search term. Twitter users using the service via the Twitter mobile app also have the option of saving searches that they have performed. A user can delete such saved searches at any time.

202. A Twitter user can also join or create "Lists" of other Twitter accounts. These Lists often organize Twitter accounts by group, topic, or interest. Viewing a timeline of a specific List will show you a stream of Tweets made only by accounts that are on that List. Users can pin their favorite lists to their Twitter Home timeline page. Twitter users have the ability to remove their accounts from Lists upon which it may appear.

203. Twitter also offers a functionality called "Spaces," which it calls "a new way to have audio conversations on Twitter." Any user can create a Space; that user is referred to as the "host." Spaces are public, so anyone can join and listen to the conversation within a Space once it is created, although a user can send another Twitter user a link to their Space and invite them to join. By default, the only individuals permitted to speak in a Space are the individuals that the host invites to do so, although this setting can be modified to allow a broader set of individuals to speak. Up to 13 people can be in a Space at a given time.

204. Twitter also offers the ability to sign into third-party apps and websites using one's Twitter account. Typically, the third-party app or website will have a link that enables the user to sign into the third-party service using their Twitter account. Doing so grants the third-party service access to the Twitter user's account. Depending on the authorizations the Twitter user gives to the third-party service, the third-party service may be able to read the user's Tweets, see who the user follows on Twitter, post Tweets to the user's profile, or access the user's email address. A user can revoke a third-party app or website's authorization to access their Twitter account and associated data at any time.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

205. Twitter collects and retains information about a user's use of the Twitter service, to include: (1) content of and metadata relating to Tweets and Direct Messages; (2) photos, images, and videos that are shared via Twitter and stored in the user's Media Timeline; (3) the identity of the accounts that a user follows and the accounts that follow the user's account; (4) the content uploaded to a user's profile page, including their avatar, banner image, and bio; (5) information about Tweets the account has liked; (6) information about Lists associated with the account; (7) information about the Spaces that a user has participated in, including the host of the Space, its start and end times, and information about other attendees; and (8) applications that are connected to the Twitter account. Twitter also collects and retains various other data about a user and his/her activity, including:

a. logs of Internet Protocol ("IP") addresses used to login to Twitter and the timestamp associated with such logins;

b. transactional records reflecting, for example, when a user changed their display name or email address;

c. the identities of accounts that are blocked or muted by the user; and

d. information relating to mobile devices and/or web browsers used to access the account, including a Twitter-generated identifier called a UUID that is unique to a given device.

206. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

207. Additionally, providers of electronic communications services and remote computing services often collect and retain user-agent information from their users. A user agent string identifies, among other things, the browser being used, its version number, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

details about the computer system used, such as operating system and version. Using this information, the web server can provide content that is tailored to the computer user's browser and operating system.

208. In my training and experience, evidence of who was using a Twitter account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

209. Based on my training and experience, direct messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Twitter account may provide direct evidence of the offenses under investigation and can also lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

210. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Twitter can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geolocation, date and time) may be evidence of who used or controlled the account at a relevant time. Similarly, device identifiers and IP addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

211. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

212. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence.

213. Therefore, Twitter's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Twitter. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

BACKGROUND CONCERNING GOOGLE[12]

214. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

215. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when

[12] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

they first turn on the device, and a Google Account is required for certain functionalities on these devices.

216. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

217. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below:

a. Email. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google.

b. Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

c. Calendar. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Contacts.

d. Maps. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

e. Messaging. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user has not disabled that feature or deleted the messages, though other factors may also impact retention.

f. Cloud Storage. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

g. Photos. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

h. Web Browser. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

browser settings may be saved to their Google Account in a record called My Activity.

218. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

219. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

220. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

221. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

222. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

223. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

224. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

225. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

226. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation, such as banking institutions used by the target or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

227. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Sections I of Attachments B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Sections II to that same Attachment.

ANDREW CROPCHO, Affiant
Special Agent, Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit on the 6th day of April, 2022.

THE HONORABLE PAULA L. McCANDLIS
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with 3 Facebook accounts that is stored at premises controlled by Meta Platforms, Inc.	)	Case No. MJ22-136 (2)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-2, incorporated herein by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B-2, incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before April 20, 2022 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any U.S. Magistrate Judge in the WDWA .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: April 6, 2022, at 10:30am

Paula L McCandlis
Judge's signature

City and state: Seattle, Washington

Hon. Paula L. McCandlis, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-2

This warrant applies to information associated with the followings Facebook accounts (the "Facebook Accounts")

ID Number:

1. **1626067687446970**
2. **100002183784122**
3. **1764433774**

Vanity Name:

1. **HashFlareGlobal**
2. **turygin**
3. **sergei.pt**

that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-2

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc.:

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A-2:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the Facebook Account and all other documents showing the user's posts and other Facebook activities **from January 1, 2014, to the present**;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them **from January 1, 2014, to the present**, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(f) All other records and contents of communications and messages made or received by the user **from January 1, 2014, to the present**, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) All past and present lists of friends created by the Facebook Account;

(l) All records of Facebook searches performed by the account **from January 1, 2014, to the present**;

(m) All information about the user's access and use of Facebook Marketplace;

(n) The types of service utilized by the user;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(q) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 1343 (Wire Fraud) and Title 18, United States Code, Section 1956, and occurring after April 2015, for each of the Facebook Accounts listed on Attachment A-2, pertaining to the following matters:

a. Items, records, or information related to the operation of a cryptocurrency cloud mining Ponzi scheme;

b. Items, records, or information related to cryptocurrency mining, the advertisement, manufacture and sale of mining equipment, or the advertisement and sale of cloud mining contracts;

c. Items, records, or information related to the termination of mining contracts and the profitability of cloud mining;

d. Items, records, or information related to purchases of cloud mining equipment, including communications with the companies Jeltan Trading, Dalmeron Projects, Dalmeron Invest, Keleta UAB, Bitmain, Bitfury, and Inno3d;

e. Items, records, or information related to the transfer, purchase, sale, or disposition of cryptocurrency;

f. Items, records, or information related to communications with HASHFLARE or HASHCOINS investors, including complaints by investors or requests for return of funds;

g. Items, records, or information related to the advertisement of HASHFLARE or HASHCOINS' services;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. Items, records, or information related to the owners, operators, employees, locations, assets, and business purpose of the companies HASHCOINS OU, HASHCOINS TRADE OU, HASHCOINS LP, HASHFLARE LP, Burfa Capital OU, Burfa Media OU, Burfa Real Estate OU, Burfa Tech OU, Burfa Trade OU, Burfa Invest OU, Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, Polybius Fintech MidCo OU, Dalmeron Projects LP, Jeltan Trading, Dalmeron Invest, Keleta UAB, and OSOM Finance (collectively, the "SUBJECT ENTITIES");

i. Items, records, or information related to the use, creation, or operation of the "SUBJECT ENTITIES," including business plans and strategies, and the anticipated success, failure, or general validity thereof;

j. Items, records, or information related to the operation of hashflare.io, burfa.com, polybius.io, dalmeron.com, or hashcoins.com;

k. Items, records, or information concerning financial transactions associated with the operation of the SUBJECT ENTITIES, including bank accounts held by the SUBJECT ENTITIES, transfers of funds by the SUBJECT ENTITIES, expenditures of money or wealth, bank statements and other financial statements, and cryptocurrency holdings;

l. Items, records, or information related to cryptocurrency mining groups, cryptocurrency public keys or addresses, cryptocurrency private keys, representations of cryptocurrency wallets or their constitutive parts, to include "recovery seeds" and "root keys," which may be used to regenerate a wallet.

m. Items, records, or information related to the salaries or earnings of individuals employed by the SUBJECT ENTITIES.

n. Items, records, or information related to the payment or calculation of recruitment bonuses paid to HASHFLARE and HASHCOINS investors.

o. Items, records, or information related to receipt of investor money, including the amount, purpose of the investment, and plans for spending that money.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

p. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.

q. Evidence indicating the account owner's state of mind as it relates to the crime under investigation.

r. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970